Oracle® Communications Charging Traffic Monitor

Installation and System Administration Guide

Release 12.1

E80470-01

March 2017

ORACLE®

Oracle Communications Charging Traffic Monitor Installation and System Administration Guide, Release 12.1

E80470-01

Contents

7 Charging Traffic Monitor Reference

Preface

This guide consists of two parts:

- Part I provides instructions for installing Oracle Communication Charging Traffic Monitor.
- Part II describes how to administer, configure, and troubleshoot Oracle Communications Charging Traffic Monitor.

Audience

- Part I is written for experienced system administrators and database administrators who install and configure networks and are familiar with operating system commands and network management.
- Part II is written for experienced system administrators and database administrators who are responsible for administering and managing networks and configuring databases and Oracle WebLogic Server.

Related Documents

Charging Traffic Monitor requires Oracle Database 12*c* Enterprise Edition, Oracle WebLogic Server 12*c*, Oracle Java 8, and Oracle Linux 7.2. See the following documentation for these products for installation and configuration instructions:

- *Oracle Database Installation Guide 12c release for Linux*
- *Oracle Java Platform Standard Edition Server JRE 8 Installation for Linux Platforms*
- *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*
- *Oracle Linux 7 Installation Guide*

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Document Revision History

The following table lists the revision history for this document:

Version	Date	Description
E80470-01	March 2017	Initial release.

Part I

Installing Charging Traffic Monitor Components

Part I provides information on how to install the Oracle Communications Charging Traffic Monitor components. It contains the following chapters:

1

Overview of Installing Charging Traffic Monitor

This chapter provides an overview of the installation procedures for Oracle Communications Charging Traffic Monitor.

About Charging Traffic Monitor

Charging Traffic Monitor monitors and troubleshoots online charging systems (OCS), such as Oracle Communications Billing and Revenue Management Elastic Charging Engine (ECE). Charging Traffic Monitor captures the traffic between the network elements and an OCS. The messages are decoded and correlated in near real-time to generate reports, key performance indicators (KPIs), and troubleshooting information.

Overview of Charging Traffic Monitor Installed Components

During the installation process, you install and configure the following components:

- Oracle Database 12*c* Enterprise Edition.

  KPIs and other correlated data, such as transactions, are stored in Oracle Database. Oracle Database is licensed separately.

- Oracle WebLogic Server 12*c*.

  Provides an application server and J2EE container for hosting and managing Charging Traffic Monitor, such as connecting Oracle Database with the Charging Traffic Monitor application. WebLogic Server is licensed separately.

- Oracle Java 8.

  Required for the Charging Traffic Monitor processing engine and WebLogic Server.

- Oracle Linux 7.2.

  Required platform for the vCollector probe and Charging Traffic Monitor.

- vCollector probe.

  The vCollector probe locates, collects, filters, and correlates customer Diameter messages. Licensed as part of Charging Traffic Monitor.

- Apache Kafka, Ignite, Spark, and ZooKeeper.

  These Apache applications and data management services do the following:

  – The Kafka broker receives the calculated and filtered Diameter messages from the vCollector probe.

  – The Spark streaming service calculates real-time KPIs and saves them into Oracle Database. It also locates sessions of interest information and

transactions and stores them into Ignite, which is an In-Memory database.

  - At regular intervals the Spark batch service reads, processes, and saves the KPIs and sessions of interest information and transactions into Oracle Database.

  Provided as RPM service files in the Charging Traffic Monitor software package.

- Charging Traffic Monitor.

  Provided as part of the Charging Traffic Monitor software package.

These components are installed on two servers creating three main areas, as shown in Figure 1–1:

- Server 1.

  Contains the Diameter message collection area (Area 1), which collects, filters, and correlates the customer Diameter messages. The vCollector probe is installed on this server.

- Server 2.

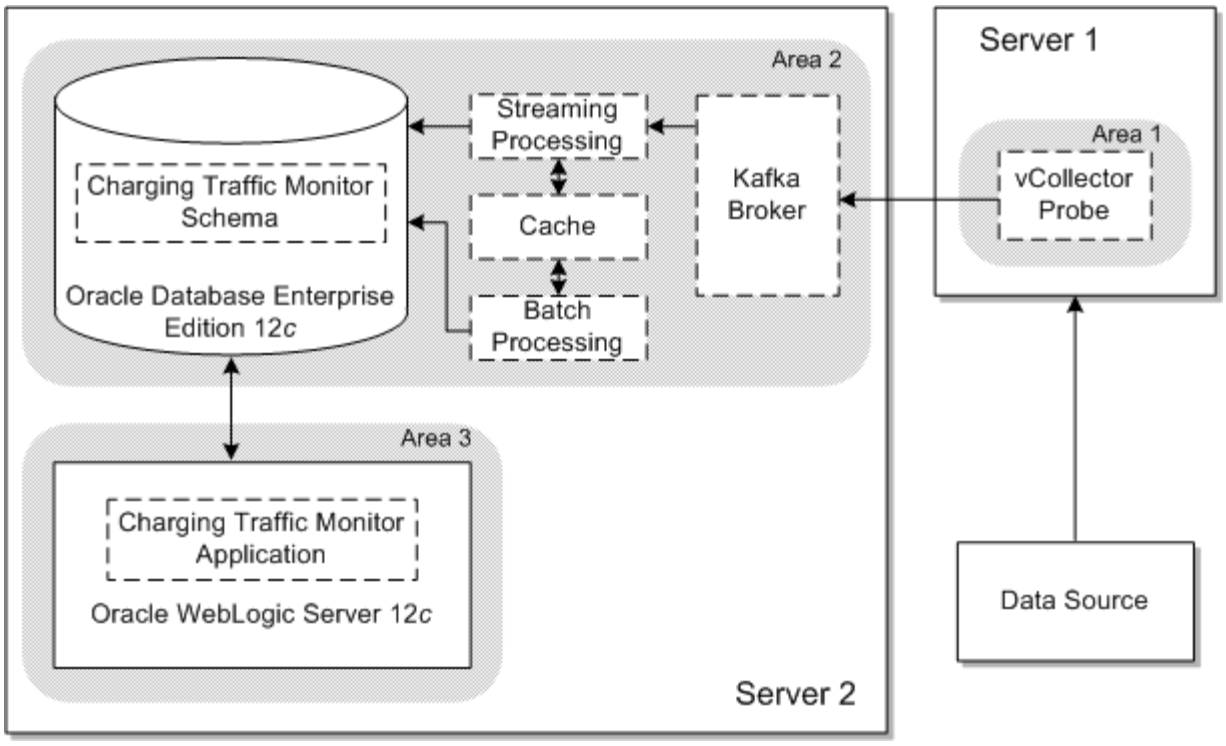
  Contains the Charging Traffic Monitor processing engine (Area 2), which receives the filtered and correlated Diameter messages from the vCollector probe, processes, and then stores the resulting KPIs and sessions of interest information and transactions in Oracle Database. The following components are installed on this server for this area:

  - Apache Kafka, Ignite, Spark, and ZooKeeper.
  - Oracle Database.

  Contains the Front End unit (Area 3), which pulls the KPI sessions of interest results as required and displays them in the Charging Traffic Monitor user interface. The following components are installed on this server for this area:

  - Oracle WebLogic Server.
  - Charging Traffic Monitor application.

Figure 1–1 Charging Traffic Monitor System Architecture and Main Areas



Overview of Charging Traffic Monitor Installation Procedure

The installation procedure follows these steps:

1. Plan your installation. When planning your installation, do the following:
   - Determine the scale of your implementation; for example, a small development system, or a large production system.
   - Determine how many physical computers you need and which software components to install on each computer.
   - Plan the system topology; for example, how the system components connect to each other over the network.
2. Review system requirements. See "Charging Traffic Monitor System Requirements".
3. Perform the pre-installation tasks on server 1:
   a. Install Oracle Linux 7.2.
   b. Enable Diameter packet capture.
4. Perform the pre-installation tasks on server 2 in the following order:
   a. Install Oracle Linux 7.2.
   b. Install and configure Oracle Database 12*c* Enterprise Edition.
   c. Install Oracle Java 8.
   d. Install and configure Oracle WebLogic Server 12*c*.
5. Install the vCollector probe on server 1.

6. Install Charging Traffic Monitor on server 2.
7. Perform the post-installation configuration tasks and secure connection tasks.

Ensuring a Successful Charging Traffic Monitor Installation

The Charging Traffic Monitor installation should be performed only by qualified personnel. You must be familiar with the Oracle Linux operating system, Oracle Java, and with Oracle WebLogic Server. You should be experienced with installing Red Hat Package Manager (RPM) packages. Oracle recommends that the Oracle Database installation and configuration be performed by an experienced database administrator.

To ensure that the Charging Traffic Monitor installation is successful, follow these guidelines:

- As you install each component (for example, the Oracle Database and WebLogic Server), verify that the components are installed successfully before continuing the installation process.
- Pay close attention to the system requirements. Before you begin installing Charging Traffic Monitor, ensure that your system has the required base software. In addition, ensure that you know all the required configuration values, such as host names and port numbers.
- As you create new configuration values, write them down. In some cases, you might need to re-enter configuration values later in the procedure.

Directory Placeholders Used in This Guide

The following placeholders listed in Table 1–1 are used in this guide to refer to the directories that contain Charging Traffic Monitor system components. For example, *Oracle_home* is the directory in which Oracle Database is installed.

Table 1–1 Directory Placeholders

Placeholder Name	Description
ctm_ip_address	The IP address of the server that hosts Oracle Database and WebLogic Server.
ctm_server_name	The host name of the server that hosts Oracle Database and WebLogic Server.
domain_home/ctmdomain	The full path to the Charging Traffic Monitor directory that contains all the files, such as configuration and scripts, for the domain in which Charging Traffic Monitor is installed.
ERR_table	The name of an Oracle Database ERR table.
Oracle_home	The directory in which Oracle Database is installed.
oracle_sid_name	The Oracle Database system identifier (SID) value entered for the ORACLE_SID environment variable in the **ctm-configuration-param** configuration file.
oracle_unique_name	The unique name for Oracle Database.
rel_num	The current release number of Charging Traffic Monitor.
service_name	The name of the Linux **systemd** service.
temp_dir	The directory where you download the Charging Traffic Monitor installation software.
vcollector_hostname	The host name of the server with SSH access and that hosts the vCollector probe.

Table 1–1 (Cont.) Directory Placeholders

Placeholder Name	Description
vcollector_server	Either the host name or IP address of the server with SSH access and that hosts the vCollector probe.
WL_password	The password for the user name that has WebLogic Server administrative privileges.
WL_username	The user name that has WebLogic Server administrative privileges.

2

Planning a Charging Traffic Monitor Installation

This chapter provides information for assisting you with planning your Oracle Communications Charging Traffic Monitor installation by providing best practices and rules about tests performed on Charging Traffic Monitor.

The presented results are derived from benchmark tests results performed in the lab. The assumptions in performance tables are the conditions used during benchmarking and represent a fair usage of the system. They are as close as possible to real traffic based on Charging Traffic Monitor usage experience. The results may differ for real customer traffic cases.

Overview

Charging Traffic Monitor is a network monitoring application. It monitors an online charging system (OCS), specifically the Gy and Ro interfaces between the OCS and PCEF, as defined by the 3rd Generation Partnership Project (3GPP) standard. This interface allows online credit control for service data flow based charging. Charging Traffic Monitor is designed to monitor the Diameter traffic of Oracle Communications Billing and Revenue Management Elastic Charging Engine (ECE).

When connected to the network on the Gy or Ro interfaces, Charging Traffic Monitor acquires Diameter traffic through either a Network switch with port mirroring or a Network TAP. The captured Diameter traffic is decoded and filtered by the vCollector probe. Several probes can be deployed (at least one for each OCS site). Diameter traffic is sent to a central repository where it is analyzed by the Charging Traffic Monitor mediation engine for building OCS and network performance indicators.

Transaction and session information is recorded and stored for later and deeper analysis. Charging Traffic Monitor implements automatic front end intelligent filtering. This feature is called **Of interest** session selection for troubleshooting.

vCollector Probe Performances

On an Oracle X5-2 server with 128 GB of memory with 2 HDD and 2 x Intel Xeon CPU E5-2660 v3 10-cores at 2.60 GHz processor or equivalent.

The vCollector probe maximum performances are:

- Diameter Gy or Ro traffic: 30,000 messages for each second.
- Input traffic bandwidth (traffic mixture allowed): 4 GB/s.

Charging Traffic Monitor Centralized Engine Performances

On an Oracle X5-2 server with 256 GB of memory with 4 HDD and 2 x Intel Xeon E5-2699 v3 18-cores 2.3 GHz processor or equivalent.

The Charging Traffic Monitor centralized engine maximum performances are:

- Diameter Gy or Ro traffic: 15,000 transactions for each second.
- Concurrent simultaneous sessions: 25 Million.
- Ratio **Of interest** session / Total sessions: 5%.

Annex 1: vCollector Probe Bill Of Materials (Oracle X6-2)

Oracle X6-2 is available in AC only (Netra X5-2 can be used for DC NEBS acquisition).

There are two options for traffic acquisition:

- One for an acquisition of 1G/10G traffic on RJ45 copper links.
- One for an acquisition of 1G/10G traffic on optical fiber links.

This affects the acquisition ports and not the port to the centralized Charging Traffic Monitor engine.

Configuration allows up to four ports in addition to one standard port (1G/10G RJ45) for the network connection to the centralized Charging Traffic Monitor engine.

Table 2–1 lists the vCollector probe 1G/10G on RJ45 copper interfaces Bill of Materials (BOM).

Table 2–1 vCollector Probe BOM with 1G/10G RJ45 copper acquisition interfaces

Oracle SKU	Description	Quantity (AC only)
7113252	Oracle Server X6-2: 1 RU base chassis with motherboard, internal 12 GB SAS RAID HBA, 2 PSUs, slide rail kit, and cable management arm.	1
7113239	One Intel Xeon E5-2630 v4 10-core 2.2 GHz processor.	2
7110350	Heat sink for 1U.	2
7113240	One 16 GB DDR4-2400 registered DIMM.	8
7110339	Eight 2.5 inch drive slots, 1 DVD-RW drive slot and disk cage for 1U.	1
7111107	One 1.2 TB 10000 rpm 2.5-inch SAS-3 HDD with marlin bracket.	2
7110359	DVD filer panel.	1
7102748	PCIe filler panel.	1
7100563	Sun Dual Port 10GBase-T Adapter (required if more than two captures ports are required).	0/1/2
6331A-N	2.5-inch HDD filler panel.	6

Table 2–2 lists the vCollector probe 1G/10G fiber SFP+ interfaces BOM.

Table 2–2 vCollector Probe BOM with 1G/10G fiber SFP+ acquisition interfaces

Oracle SKU	Description	Quantity (AC only)
7113252	Oracle Server X6-2: 1 RU base chassis with motherboard, internal 12 GB SAS RAID HBA, 2 PSUs, slide rail kit, and cable management arm.	1
7113239	One Intel Xeon E5-2630 v4 10-core 2.2 GHz processor.	2
7110350	Heat sink for 1U.	2
7113240	One 16 GB DDR4-2400 registered DIMM.	8
7110339	Eight 2.5 inch drive slots, 1 DVD-RW drive slot and disk cage for 1U.	1
7111107	One 1.2 TB 10000 rpm 2.5-inch SAS-3 HDD with marlin bracket.	2
7110359	DVD filer panel.	1
7102748	PCIe filler panel.	1
1109A-Z	ASSY, 2X10 GbE SFP+, X8PCIe 2.0, LP, Lead Free (Niantic).	1/2
6331A-N	2.5-inch HDD filler panel.	6

In addition, SFP(+) modules according to the network type shall be ordered.

Each acquisition card has 2 SFP(+) slots and 2 cards for each server.

Total: 4 SFP+ acquisition ports for the server.

Important: A USB flash drive (8 GB) will be required for the initial installation or disaster recovery.

In addition, two power cords shall be ordered according to the installation country or the power distribution unit installed in the frame.

Annex 2: Charging Traffic Monitor Centralized Engine Bill of Material (Oracle X6-2)

Oracle X6-2 is available in AC only (Netra X5-2 can be used for DC NEBS acquisition).

Table 2–3 lists the Charging Traffic Monitor centralized engine BOM.

Table 2–3 Charging Traffic Monitor Centralized Engine BOM

Oracle SKU	Description	Quantity (AC only)
7113252	Oracle Server X6-2: 1 RU base chassis with motherboard, internal 12 GB SAS RAID HBA, 2 PSUs, slide rail kit, and cable management arm.	1
7113235	One Intel Xeon E5-2699 v4 22-core 2.2 GHz processor.	2
7110350	Heat sink for 1U.	2
7113240	One 16 GB DDR4-2400 registered DIMM.	16
7110339	Eight 2.5 inch drive slots, 1 DVD-RW drive slot and disk cage for 1U.	1
7111107	One 1.2 TB 10000 rpm 2.5-inch SAS-3 HDD with marlin bracket.	4

Table 2–3 (Cont.) Charging Traffic Monitor Centralized Engine BOM

Oracle SKU	Description	Quantity (AC only)
7110359	DVD filer panel.	1
7102748	PCIe filler panel.	3
6331A-N	2.5-inch HDD filler panel.	4

Important: A USB flash drive (8 GB) will be required for the initial installation or disaster recovery.

In addition, two power cords shall be ordered according to the installation country or the power distribution unit installed in the frame.

Annex 3: RFC and 3GPP Compliancy Statement

Table 2–4 lists the RFC and 3GPP compliancy standards.

Table 2–4 RFC and 3GPP Standards

Standard	Description
RFC 4006	Diameter Credit-Control Application.
RFC 6733	Diameter Base Protocol.
RFC 793	Transmission Control Protocol.
RFC 4960	Stream Control Transmission Protocol.
Gy interface	Prepaid charging defined in TS 23.203, TS 32.299.
Ro interface	Charging defined in TS 32.299.

3

Charging Traffic Monitor System Requirements

This chapter describes the software, hardware, and information requirements for installing Oracle Communications Charging Traffic Monitor.

Supported Software and Hardware Requirements

You must install and connect all required software for optimal performance.

Table 3–1 lists the supported operating systems for running Charging Traffic Monitor.

Table 3–1 Supported Operating Systems

Product	Version	Notes
Oracle Linux 7 6 x86-64 (64 bit)	7.2	N/A
Oracle Linux 7 6 x86-64 (64 bit)	7.2 (with Oracle Unbreakable Enterprise Kernel for Linux)	N/A

Table 3–2 lists the minimum software and hardware requirements for running Charging Traffic Monitor.

The software and hardware requirements for your Charging Traffic Monitor installation depend on your deployment plan and the amount of data you plan to process.

For more information on the software and hardware requirements for Oracle Database 12*c* Enterprise Edition and Oracle WebLogic Server 12*c*, see the documentation for those products.

Table 3–2 Supported Software and Hardware Requirements

Product	Version	Requirements
Oracle Communications Charging Traffic Monitor	12.1	■ 2 CPUs x18 cores, 256 GB RAM. ■ Minimum of 2 x 1.2 TB HDD disks and 2 x 400 GB solid state drives (SSD).
Oracle Database 12*c* Enterprise Edition	12.1.0.2	■ x86_64 16 cores, 128 GB physical memory. Minimum of 12 disks (600 GB minimum for each disk). Disks must be installed in RAID 10 configuration. ■ (Required) Oracle Online Analytical Processing. ■ Oracle Data Mining. ■ (Optional) In memory.
Oracle Java Platform	8	All Java 8 versions are supported. Oracle recommends that you install the latest available version and security update.
Oracle WebLogic Server 12*c*	12.1.3.0.0	Oracle recommends that you install this version of WebLogic Server 12*c* for Charging Traffic Monitor. See *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.
VCollector Probe	12.1	■ 2 CPUs x 10 cores, 128 GB RAM. ■ Minimum of 2 disks (600 GB minimum for each disk).

Supported Internet Browsers

The following Internet browsers are supported:

- Microsoft Internet Explorer (Windows OS), version 11+.
- Mozilla Firefox (Windows, OEL, RHEL), version Firefox ESR 38+.
- Google Chrome (Windows, Mac, OEL, RHEL), version Chrome 39+.

Information Requirements

This section describes the configuration entry values and the environment variable values that you will be required to provide during the Charging Traffic Monitor installation. These configuration values are defined when installing Oracle Database 12*c*, Oracle Java, and Oracle WebLogic Server 12*c*.

Oracle Database Connection Information

Table 3–3 lists the Oracle Database configuration entry values and the environment variable values that are required during the Charging Traffic Monitor installation.

Table 3–3 Oracle Database Information

Prompt / Environment Variable	Description	Value Obtained from Pre-Installation
Enter Oracle database 'CTM' user password:	The password that was used to install Oracle Database. Provided during the installation of Oracle Database.	-
Enter Oracle database wallet password:	The password for the Oracle Database user name that has Oracle wallet privileges. Provided during the creation of an Oracle wallet.	-
Enter sys (oracle database sysadm) password:	(Optional) The password for the user name that has full SYSDBA privileges for remote database access. **Note:** If a value is not entered for the ORACLE_DB_SYSDBA_USER environment variable then this value will not be requested. Provided during the creation of the Oracle Database instance.	-
ORACLE_BASE	The root path and directory in which Oracle Database is installed. This directory contains the Oracle Database software and directories, such as, **bin**, **rdbms**, and **sqlplus**. Provided during the installation of Oracle Database.	-
ORACLE_HOME	The path and directory in which Oracle Database is installed. This directory is a subdirectory of ORACLE_BASE containing the installed files and files such as, registry entries, net service names, program groups, and the PATH variable. Provided during the installation of Oracle Database.	-
ORACLE_SID	The Oracle System identifier (SID), which is a unique name for identifying a database on a system. Provided during the creation of the Oracle Database instance.	-
ORACLE_PDB	The Oracle pluggable database (PDB) name, which contains the Charging Traffic Monitor portable schemas, schema objects, and non schema objects. **Important:** This value must be the *connection_name* value that you entered in the **tnsnames.ora** configuration file. For more information, see "Adding a Connect Descriptor Name for a Pluggable Database". Provided during the creation of the Oracle Database instance.	-
ORACLE_DB_PORT	The listening port number of Oracle Database. Provided during the installation of Oracle Database.	-
ORACLE_DB_HOST	The host name for the server that hosts Oracle Database. Provided during the installation of Oracle Database.	-
ORACLE_DB_LOCAL_USER	The user name that has full SYSDBA privileges for local database access. **Note:** If a value is entered, a value is not required for the ORACLE_DB_SYSDBA_USER environment variable.	-
ORACLE_DB_USER	The user name that was used to install Oracle Database.	-

Table 3–3 (Cont.) Oracle Database Information

Prompt / Environment Variable	Description	Value Obtained from Pre-Installation
ORACLE_WALLET_PATH	The path to the Oracle wallet directory, where your Charging Traffic Monitor Oracle wallet files are stored. Provided during the creation of an Oracle wallet.	-
ORACLE_WALLET_ADMIN	The path to the directory that contains the **sqlnet.ora** and the **tnsnames.ora** files. Provided during the creation of an Oracle wallet.	-
TNS_ADMIN	The path and directory in which the SQL *NET configuration files are stored, such as **sqlnet.ora** and **tnsnames.ora**. **Note:** This environment variable locates Oracle wallets. Provided during the creation of the Oracle Database instance.	-
ORACLE_DB_SYSDBA_USER	(Optional) The user name that has full SYSDBA privileges for remote database access. **Note:** If a value is entered, a value is not required for the ORACLE_DB_LOCAL_USER environment variable. Provided during the creation of the Oracle Database instance.	-
ORACLE_DB_SSH_USER	(Optional) The secure socket shell (SSH) user name that has Oracle Database remote access privileges. If Oracle Database is not installed on the server that hosts the Charging Traffic Monitor processing engine this name is used.	-

Java Connection Information

Table 3–4 lists the Oracle Java environment variable value that is required during the Charging Traffic Monitor installation.

Table 3–4 Java Information

Environment Variable	Description	Value Obtained from Pre-Installation
JAVA_HOME	The path to the directory in which Java is installed. Provided during the installation of Java.	-

WebLogic Server Connection Information

Table 3–5 lists the WebLogic Server configuration entry values and the environment variable values that are required during the Charging Traffic Monitor installation.

Table 3–5 WebLogic Server Information

Prompt / Environment Variable	Description	Value Obtained from Pre-Installation
Enter Weblogic password:	The password for the user name that has WebLogic Server user interface portal access privileges. Provided during the installation of WebLogic Server.	-
WL_HOST	The host name for the server that hosts Oracle Database and WebLogic Server. Provided during the installation of WebLogic Server.	-
WL_USERNAME	The user name that has WebLogic Server user interface portal access privileges. Provided during the installation of WebLogic Server.	-
WL_DOMAIN	The WebLogic Server **domains** directory name. Provided during the installation of WebLogic Server.	-
WL_DOMAIN_DIR	The full path to the WebLogic Server **domains** directory. Provided during the installation of WebLogic Server.	-
WL_PORT	The listening port number of the WebLogic Server administrative instance. Provided during the installation of WebLogic Server.	-
WL_HOME	The path to the directory in which WebLogic Server is installed. Provided during the installation of WebLogic Server.	-
WL_TARGET	The name of the WebLogic Server administrative server instance. Provided during the installation of WebLogic Server.	-
WL_SSH_USER	(Optional) The SSH user name that has WebLogic Server remote access privileges. If WebLogic Server is not installed on the server that hosts the Charging Traffic Monitor processing engine this name is used. Provided during the installation of WebLogic Server.	-

4

Charging Traffic Monitor Pre-Installation Tasks

This chapter describes the tasks that you perform before installing Oracle Communications Charging Traffic Monitor.

Before starting the pre-installation tasks in this chapter, read the following:

- Overview of Installing Charging Traffic Monitor
- Planning a Charging Traffic Monitor Installation
- Charging Traffic Monitor System Requirements

Creating Your Charging Traffic Monitor System Architecture

Other Oracle products and third-party software are involved in building the Charging Traffic Monitor system architecture. For more information on the Charging Traffic Monitor system architecture see "Overview of Charging Traffic Monitor Installed Components".

Before installing Charging Traffic Monitor, do the following pre-installation tasks in the following order:

1. Prepare the server that will host the vCollector probe as follows:
    a. Install and configure the Oracle Linux operating system. For more information, see "Installing and Configuring Oracle Linux".
    b. Enable Diameter packet capture. For more information, see "Enabling Online Charging System Diameter Traffic Capture".
2. Prepare the server that will host the Charging Traffic Monitor application and processing engine.
    a. Install and configure the Oracle Linux operating system. For more information, see "Installing and Configuring Oracle Linux".
    b. Install and configure Oracle Database. For more information, see "Installing and Configuring Oracle Database".
    c. Install and configure Oracle Java 8. For more information, see "Installing and Configuring Java".
    d. Install and configure Oracle WebLogic Server. For more information, see "Installing and Configuring WebLogic Server".

Installing and Configuring Oracle Linux

Install the Oracle Linux operating system on both the server that will host the vCollector probe and the server that will host the Charging Traffic Monitor application.

During the installation of Oracle Linux do the following:

- Configure the host name of the server.
- Configure the IP address, the Network gateway address, and the netmask of the server.
- Enable the Network Time Protocol (NTP) time source IP address of the server.
- Set the time zone of the server.
- On the server that will host Charging Traffic Monitor, whilst you are configuring disk partitioning set the swap file size.

For complete installation instructions and general information about installing and configuring Oracle Linux, see the Oracle Linux documentation.

Enabling Online Charging System Diameter Traffic Capture

The server that will host the vCollector probe must have access to your Diameter transactions.

To enable online charging system (OCS) Diameter traffic capture:

1. Connect the server that hosts your OCS and the server that will host the vCollector probe with one of the following computer networking devices:
   - Network Switch.
   - Network Tap.
2. Configure OCS transmitted and received Diameter traffic as follows:
   - For a Network Switch:
     a. Enable port mirroring.
     b. Configure the capture of all Diameter traffic. The network switch interface must be set in promiscuous mode, which avoids filtering on the Ethernet MAC address.

     For installation, port mirroring, and configuration instructions, see your Network Switch documentation.
   - For a Network Tap:

     Configure the capture of all Diameter traffic. The network tap interface must be set in promiscuous mode, which avoids filtering on the Ethernet MAC address

     For installation and configuration instructions, see your Network Tap documentation.

Installing and Configuring Oracle Database

Before installing Oracle Database do the following:

1. On the server that will host the Charging Traffic Monitor application and processing engine, verify that you can access the Yellowdog Updater Modified

(YUM) utility, which is provided with Oracle Linux. For more information on the YUM utility, see the Oracle Linux documentation.

2. Verify that you have a utility for extracting compressed files. If not do the following:

   To install the **unzip** utility, run the following:

   ```
   yum install unzip
   ```

3. During the Oracle Database installation you will be required to select a partition in which to install Oracle Database. Verify your Diameter data storage requirements so that you select a partition large enough for storing your Diameter data.

   Important: Do not install Oracle Database under the root partition as this partition has limited storage space.

Install Oracle Database on the server that will host the Charging Traffic Monitor application and processing engine.

For complete installation instructions and general information about installing and configuring Oracle Database, see *Oracle Database Installation Guide 12c release for Linux*.

Oracle recommends that the installation and configuration of Oracle Database be preformed by an experienced database administrator.

Important: Oracle Database and pluggable databases must be configured to restart all Charging Traffic Monitor resources automatically when the server is rebooted. For more information on how to automate an Oracle Database restart, see "Automating Oracle Database Shutdown and Startup with a Linux Service Script".

Recording Oracle Database Information

Some of the information that you set when installing Oracle Database will be required during the Charging Traffic Monitor installation. Record this information in Table 3–3 of "Charging Traffic Monitor System Requirements" and provide it to your Charging Traffic Monitor installer. For example:

- Oracle Database BASE directory name.
- The path to the directory in which Oracle Database is installed.
- Oracle Database service name.
- Oracle pluggable database (PDB) name.
- Oracle Database server port number.
- Oracle Database server host name.
- The path and directory in which the **sqlnet.ora** and **tnsnames.ora** files are located.
- User name that has full SYSDBA privileges.
- Password for the user name that has full SYSDBA privileges.
- The Oracle Database user name that has Oracle wallet privileges.
- The password for the Oracle Database user name that has Oracle wallet privileges.
- The path to the Oracle wallet directory.

- (Remote Access Only) The secure socket shell (SSH) user name that has Oracle Database remote access privileges.

Adding a Connect Descriptor Name for a Pluggable Database

The connection credentials for Charging Traffic Monitor and Charging Traffic Monitor components, including your Oracle Database connection credentials are stored in an Oracle wallet.

The Oracle Database **tnsnames.ora** configuration file hides the details of the Oracle Database network connection string address details by using an alias. This alias maps the database network address in a connect descriptor, which is used in the Oracle wallet.

If you are installing Charging Traffic Monitor on a pluggable database (PDB), the PDB network connection string address detail alias and the details of the pluggable database must be added into the **tnsnames.ora** configuration file.

To add a connect descriptor name for a pluggable database:

1. Log in to the server that hosts the Oracle Database with the user name and password that was used to install Oracle Database.
2. Open the *Oracle_home*/**network/admin/tnsnames.ora** configuration file, where *Oracle_home* is the directory in which Oracle Database is installed.

   If a **tnsnames.ora** file does not exist, create one.
3. Search for or add the following lines if not present:

```
connection_name =
   (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = host_name)(PORT = port_number))
      (CONNECT_DATA =
         (SERVER = DEDICATED)
         (SERVICE_NAME = service_name)
       )
   )
```

4. Update as follows:
   - Replace *connection_name* with the PDB network connection string address detail alias name.

     Important: The *connection_name* value must be the value you enter for the ORACLE_PDB environment variable value in the **ctm-configuration-param** configuration file. For more information, see "ctm-configuration-param Configuration File Environment Variables".
   - Replace *host_name* with the Oracle Database host name.
   - Replace *port_number* with the Oracle Database listener port number.
   - Replace *service_name* with the Oracle PDB Database service name.
5. Save the file.

Installing and Configuring Java

Install Oracle Java 8 on the server that will host the Charging Traffic Monitor application and processing engine.

For complete installation instructions and general information about installing and configuring Java, see the Oracle Java documentation.

Java Information You Need to Record

Some of the information that you set when installing Java will be required during the Charging Traffic Monitor installation. Record the following information in Table 3–4 of "Charging Traffic Monitor System Requirements" and provide it to your Charging Traffic Monitor installer:

- The path to the directory in which Java is installed.

Installing and Configuring WebLogic Server

Install Oracle WebLogic Server on the server that will host the Charging Traffic Monitor application and processing engine.

Note: During installation you must choose between a **Production** or a **Development** environment. If you choose a **Production** environment, when WebLogic Server is started automatically you must enter a login name and password. For more information on how to prevent adding a user name and password when WebLogic Server is started automatically, see "Automating WebLogic Server Shutdown and Startup with a Linux Service Script".

For complete installation instructions and general information about installing and configuring WebLogic Server and a WebLogic Server domain, see *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

Important: WebLogic Server must be configured to restart automatically when the server is rebooted. For more information on how to automate a WebLogic Server restart, see "Automating WebLogic Server Shutdown and Startup with a Linux Service Script".

WebLogic Server Information You Need to Record

Some of the information that you set when installing WebLogic Server will be required during the Charging Traffic Monitor installation. Record this information in Table 3–5 of "Charging Traffic Monitor System Requirements" and provide it to your Charging Traffic Monitor installer. For example

- User name that was used to install WebLogic Server.
- The host name for the server that hosts Oracle Database and WebLogic Server.
- User name that has WebLogic Server user interface portal access privileges.
- Password for the user name that has WebLogic Server user interface portal access privileges.
- The path to the WebLogic Server **domains** directory.

- The listening port number of the WebLogic Server administration instance.
- The path to the directory in which WebLogic Server is installed.
- The name of the WebLogic Server administrative server instance.
- (Remote Access Only) The secure socket shell (SSH) user name that has Oracle Database remote access privileges.

5

Installing Charging Traffic Monitor

This chapter describes how to install Oracle Communications Charging Traffic Monitor.

Before installing Charging Traffic Monitor, read the following:

- Overview of Installing Charging Traffic Monitor
- Planning a Charging Traffic Monitor Installation
- Charging Traffic Monitor System Requirements
- Charging Traffic Monitor Pre-Installation Tasks

About Installing Charging Traffic Monitor

Charging Traffic Monitor requires the use of other Oracle software and third-party software. Before installing Charging Traffic Monitor, verify that the Charging Traffic Monitor pre-install tasks have been completed. For more information, see "Charging Traffic Monitor Pre-Installation Tasks".

Install Charging Traffic Monitor in the following order:

1. Install Charging Traffic Monitor on the server that hosts Oracle Database and Oracle WebLogic Server. This does the following:
   - Installs the Apache components and creates the key performance indicator (KPI) processing unit (Charging Traffic Monitor engine).
   - Installs the Charging Traffic Monitor schema in Oracle Database.
   - Creates an Oracle wallet.
   - Adds the Charging Traffic Monitor application.
   - Creates a web container.
   - Creates the Charging Traffic Monitor **ctmgrp** group name and the **ctmusr** user name on the Linux operating system.
   - Creates the Charging Traffic Monitor **ctm-group** group name for WebLogic Server.
   - Creates a Charging Traffic Monitor user interface on the WebLogic Server application server.

   For installation procedures, see "Installing Charging Traffic Monitor on the Server that Hosts Oracle Database and WebLogic Server".
2. Install the vCollector probe on an Oracle Linux platform server with secure socket shell (SSH) access.

This installs the vCollector probe and other related software and configuration files.

For installation procedures, see "Installing the vCollector Probe on a Server with SSH access".

3. Complete the Charging Traffic Monitor post-installation tasks.

   For more information, see "Charging Traffic Monitor Post-Installation Tasks".

Installing Charging Traffic Monitor on the Server that Hosts Oracle Database and WebLogic Server

This section describes the Charging Traffic Monitor installation procedures. The Charging Traffic Monitor installation must be run by the Oracle Linux **root** user.

To install Charging Traffic Monitor on the server that hosts Oracle Database and WebLogic Server:

1. Log in to the server that hosts Oracle Database and WebLogic Server as the **root** user.
2. Verify that the Oracle Linux version 7.2 platform is installed by running the following:

   ```
   cat /etc/oracle-release
   ```

3. Verify that Oracle Database is installed and the pre-installation steps are completed. For more information, see "Installing and Configuring Oracle Database".
4. Verify that Oracle Java is installed and the pre-installation steps are completed. For more information, see "Installing and Configuring Java".
5. Verify that WebLogic Server is installed and the pre-installation steps are completed. For more information, see "Installing and Configuring WebLogic Server".
6. Download the Charging Traffic Monitor application software by doing the following:
   a. Create a temporary directory (*temp_dir*) on the server that hosts Oracle Database and WebLogic Server.
   b. Go to the Oracle Software Delivery web site:

      https://edelivery.oracle.com/

   c. Read and accept the **License Agreement** and **Export Restrictions** and click **Continue**.
   d. Download the Charging Traffic Monitor application **ctm-***rel_num***.zip** file to the *temp_dir*. Where *rel_num* is the current release number of Charging Traffic Monitor. For example, **ctm-12.1.0.0.0.zip**.
   e. Unzip the Charging Traffic Monitor application **ctm-***rel_num***.zip** file.
   f. Verify that the **ctm-***rel_num***.x86_64.rpm** Red Hat Package Manager (RPM) file is present.
7. Install Charging Traffic Monitor by running the following command:

   ```
   rpm -ivh temp_dir/ctm-*.x86_64.rpm
   ```

Where *temp_dir* is the path and directory in which you unzipped the Charging Traffic Monitor RPM files.

Charging Traffic Monitor is installed.

For information on the Charging Traffic Monitor configuration tasks, see "Configuring Charging Traffic Monitor".

Installing the vCollector Probe on a Server with SSH access

This section describes the vCollector probe installation procedures. The vCollector probe installation must be run by the Oracle Linux **root** user.

To install the vCollector probe on a server with secure socket shell (SSH) access:

1. Log in to the server with SSH access as the **root** user.
2. Verify that the Oracle Linux version 7.2 platform is installed by running the following:

   ```
   cat /etc/oracle-release
   ```

3. Download the vCollector probe software by doing the following:
   a. Create a temporary directory (*temp_dir*) on the server with SSH access.
   b. Go to the Oracle Software Delivery web site:

      https://edelivery.oracle.com/

   c. Read and accept the **License Agreement** and **Export Restrictions** and click **Continue**.
   d. Download the vCollector probe **ctm-vcollector-***rel_num***.zip** file to the *temp_dir*. Where *rel_num* is the current release number of Charging Traffic Monitor. For example, **ctm-vcollector-12.1.0.0.0.zip**.
   e. Unzip the vCollector probe **ctm-vcollector-***rel_num***.zip** file.
   f. Verify with the **ls** command that the following RPM files are present:
      - avrocpp-*rel_num*.x86_64.rpm
      - librdkafka-*rel_num*.x86_64.rpm
      - libsodium-*rel_num*.x86_64.rpm
      - openpgm-*rel_num*.x86_64.rpm
      - protobuf-*rel_num*.x86_64.rpm
      - protobuf-python-*rel_num*.x86_64.rpm
      - python-zmq-*rel_num*.x86_64.rpm
      - vcollector-*rel_num*.x86_64.rpm
      - zeromq-*rel_num*.x86_64.rpm
      - zeromq3-*rel_num*.x86_64.rpm

      Note: The vCollector probe **ctm-vcollector-***rel_num***.zip** file also contains Oracle RPM files for Oracle Linux.

4. Install the vCollector probe RPM files by running the following command:

```
yum install -y temp_dir/*.rpm
```

Where *temp_dir* is the path and directory in which you unzipped the vCollector probe RPM files.

The vCollector probe for Charging Traffic Monitor is installed.

For information on the vCollector probe configuration tasks, see "Configuring the vCollector Probe".

Charging Traffic Monitor Post-Installation Tasks

This section provides instructions for the post-installation tasks for Charging Traffic Monitor.

Complete the Charging Traffic Monitor post-installation tasks in the following order:

1. Complete the Charging Traffic Monitor configuration procedures.

   For configuration procedures, see "Configuring Charging Traffic Monitor".

2. Complete the vCollector probe configuration procedures.

   For configuration procedures, see "Configuring the vCollector Probe".

3. Create a secure connection between the vCollector probe and the Kafka broker.

   For more information, see "Creating a Secure Connection between the vCollector Probe and the Kafka Broker".

Configuring Charging Traffic Monitor

This section describes how to configure Charging Traffic Monitor. The Charging Traffic Monitor configuration task must be completed by the Oracle Linux **root** user.

To configure Charging Traffic Monitor:

1. Verify that Charging Traffic Monitor is installed on the server that hosts Oracle Database and WebLogic Server.
2. Log in to the server that hosts Oracle Database and WebLogic Server as the **root** user.
3. Go to **/opt/ctm/scripts** and create a backup of the **ctm-configuration-param** script file with the following command:

   ```
   cp ctm-configuration-param ctm-configuration-param.backup
   ```

4. In a text editor, open the **ctm-configuration-param** configuration script file and update with your system environment variable values and user names.

   For more information on the **ctm-configuration-param** environment variables and their descriptions, see "ctm-configuration-param Configuration File Environment Variables".

   Important: The ORACLE_PDB environment variable value must be the *connection_name* value that you entered in the **tnsnames.ora** configuration file. For more information, see "Adding a Connect Descriptor Name for a Pluggable Database".

5. Save the file.

6. Start and enable an automatic restart of the Charging Traffic Monitor services, set the Charging Traffic Monitor system environment variables, user names, passwords, and storage tablespace sizes, and create the Charging Traffic Monitor and Kafka SLL certificates by running the following command:

   ./ctm-configuration

   > **Note:** Creating the Charging Traffic Monitor **tsctm** and **tssession** tablespaces with the Oracle recommended default values is time consuming. It takes approximately 70 minutes for this Charging Traffic Monitor configuration step.

7. At the following prompt, enter the password that was used to install Oracle Database:

   ```
   Enter Oracle database 'CTM' user password:
   ```

8. If a value was entered for the ORACLE_DB_SYSDBA_USER environment variable, at the following prompt, enter the password for the user name that has full SYSDBA privileges for remote database access:

   ```
   Enter sys (oracle database sysadm)
   password:
   ```

9. At the following prompt, enter the password for the Oracle Database user name that has Oracle wallet privileges:

   ```
   Enter Oracle database wallet password:
   ```

10. At the following prompt, enter the password that protects the SSL certificate files and provides secure access:

    ```
    Enter CTM ssl certificate password (empty for ssl disabled):
    ```

    > **Important:** Oracle recommends that you secure all your SSL certificate files

    > **WARNING: If a value is not entered the Apache Kafka broker is installed without security.**

11. Do one or more of the following:

    - If logged on to the WebLogic Server console, log out.
    - If WebLogic Server is running, stop and restart WebLogic Server.
    - If WebLogic Server is not running, start WebLogic Server.

    For information on how to automate a WebLogic Server shutdown and restart, see "Automating WebLogic Server Shutdown and Startup with a Linux Service Script".

12. Deploy the Charging Traffic Monitor application **WAR** files and domain security for WebLogic Server, by running the following command:

    ./ctm-configuration-front-end

13. At the following prompt, enter the password for the user name that has WebLogic Server user interface portal access privileges:

```
Enter Weblogic password:
```

For more information on the Charging Traffic Monitor configuration of the WebLogic Server domain, see "WebLogic Server Domain Configuration".

14. Secure the WebLogic Server domain with the SSL protocol. For more information on how to secure the WebLogic Server domain with the SSL protocol and WebLogic Server keystores, see the WebLogic Server documentation.
15. Open the WebLogic Server administration console management tool and create a WebLogic Server **ctm** user as part of the **ctm-group** group. For more information about creating users within groups in the WebLogic Server administration console management tool, see the WebLogic Server documentation.

Charging Traffic Monitor is configured.

Configuring the vCollector Probe

This section describes how to configure the vCollector probe. The vCollector probe configuration task must be completed by the Oracle Linux **root** user.

> **Note:** The **rat.conf** configuration file is used by the **pld-rat** service for configuring the vCollector probe for your system. The **pld-rat** service is the vCollector probe's main processing service.

To configure the vCollector probe:

1. Verify that the vCollector probe is installed on the server with SSH access.
2. Log in to the server with SSH access and that hosts the vCollector probe as the **root** user.
3. Do one of the following:
   - If your servers are managed by a domain name system (DNS) go to step 4.
   - If your servers are not managed by DNS, run the following command:

     echo *ctm_ip_address ctm_server_name* **>> /etc/hosts**

     Where
     - *ctm_ip_address* is the IP address of the server that hosts Oracle Database and WebLogic Server.
     - *ctm_server_name* is the host name of the server that hosts Oracle Database and WebLogic Server.
4. Go to **/etc/iptego/** and create a backup of the **rat.conf** configuration file with the following command:

   ```
   cp rat.conf rat.conf.backup
   ```

5. In a text editor, open the **rat.conf** configuration file and update with your system configuration values, for example, your capture devices. For a list of available **rat.conf** parameters and their descriptions, see "rat.conf Configuration File Parameters".

> **Important:** Values that must not change are described as **Reserved for internal use. Do not change**.

6. Save the file.
7. Enable and start the vCollector probe with the following commands:

```
systemctl enable pld-rat
systemctl start pld-rat
```

> **Note:** The **systemctl** command can be run anywhere on the server as long as the user has root privileges.

8. (Optional) To check the **systemd** status of the vCollector probe run the following command:

```
systemctl status pld-rat
```

9. (Optional) To troubleshoot the vCollector probe run the **rat_mon.py** utility. For more information on using the **rat_mon.py** utility, see "Working with the vCollector Probe Troubleshooting Utility".

The vCollector probe for Charging Traffic Monitor is configured.

Creating a Secure Connection between the vCollector Probe and the Kafka Broker

A secure connection must be created between the vCollector probe and Apache Kafka with the secure sockets layer (SSL) protocol.

To create a secure connection between the vCollector probe and the Kafka broker:

1. Log in to the server with SSH access and that hosts the vCollector probe as the **root** user.
2. Create a **ctm-ssl** directory by entering the following command:

```
mkdir /root/ctm-ssl
```

3. Keep the terminal console open for the server with SSH access and that hosts the vCollector probe.
4. In a new terminal console, log in to the server that hosts Oracle Database and WebLogic Server as the **root** user.
5. Go to **/opt/ctm/scripts/** and run the following command:

```
./ctm-configuration-ssl vcollector_hostname
```

Where *vcollector_hostname* is the host name of the server with SSH access and that hosts the vCollector probe.

6. At the following prompt, enter the password that protects the SSL certificate files and provides secure access:

```
Enter CTM ssl certificate password (empty for ssl disabled):
```

> **Important:** Oracle recommends that you secure all your SSL certificate files

The vCollector probe SSL certificate and authentication files are generated.

7. Stay in the terminal console where you logged in to the server that hosts Oracle Database and WebLogic Server and go to **/root/ctm-ssl**.

8. Verify with the **ls** command that the following files were generated in step 5:
   - *vcollector_hostname*_**client.key**
   - *vcollector_hostname*_**client.pem**
   - **ca-cert**
9. Transfer the *vcollector_hostname*_**client.key**, *vcollector_hostname*_**client.pem**, and the **ca-cert** files to the **/root/ctm-ssl** directory you created on the server with SSH access and that hosts the vCollector probe in step 2, with the following command:

   ```
   scp ca-cert vcollector_hostname_client.pem vcollector_hostname_client.key
   root@vcollector_server:/root/ctm-ssl/
   ```

   Where *vcollector_server* is either the host name or the IP address of the server with SSH access and that hosts the vCollector probe, as follows:
   - If your servers are managed by a DNS, use the host name of the server with SSH access and that hosts the vCollector probe.
   - If you servers are not managed by a DNS, use the IP address of the server with SSH access and that hosts the vCollector probe.
10. Go back to the terminal console where you logged in to the server with SSH access and that hosts the vCollector probe.
11. In a text editor, open the **/etc/iptego/rat.conf** configuration file.
12. Search for the **kafka** section and update the brokers and SSL parameters as follows:
    a. For the **brokers** parameter, change the port number in the URL string to **9093**.
    b. For the **encryption** parameter, enter the protocol name that will be used for communicating with the Kafka brokers. For example, **ssl**.
    c. For the **ssl_key_pw** parameter, enter the SSL certificate's password.
    d. For the **ssl_key** parameter, enter the path and name of the client private key that is used for authentication. For example, **/root/ctm-ssl/***vcollector_hostname*_**client.key**.
    e. For the **ssl_cert** parameter, enter the path and name of the public key that is used for authentication. For example, **/root/ctm-ssl/***vcollector_hostname*_**client.pem**.
    f. For the **ssl_cas** parameter, enter the path and name of the SSL certificate. For example, **/root/ctm-ssl/ca-cert**.

    For more information on the **rat.conf** configuration file, see "rat.conf Configuration File Parameters".
13. Save and close the file.
14. Restart the **pld-rat** service by running the following command:

    ```
    systemctl restart pld-rat
    ```

15. (Optional) Verify that the connection between the vCollector probe and the Kafka broker is fully established and that data traffic is being sent from the vCollector probe by using the **rat_mon.py** utility. For more information on the rat_mon.py utility, see "Working with the vCollector Probe Troubleshooting Utility".

Part II

Charging Traffic Monitor Administration

Part II provides information on the system administration tasks for Oracle Communications Charging Traffic Monitor. It contains the following chapters:

- Administration of Charging Traffic Monitor
- Charging Traffic Monitor Reference

6

Administration of Charging Traffic Monitor

This chapter provides system administration instructions for administering Oracle Communications Charging Traffic Monitor.

Administering Charging Traffic Monitor

The Charging Traffic Monitor system administrator is responsible for the Oracle Communications Charging Traffic Monitor administration tasks.

Creating a List of Subscriber Of Interest Entries

You can identify Diameter sessions that are important for further analysis with the Charging Traffic Monitor **Of Interest** feature. This feature enables you to monitor and troubleshoot specific subscribers that could have potential issues and are out of the scope of the criteria provided by Charging Traffic Monitor (sessions that are too long or sessions that have too many transactions), or are of special interest.

To create a list of subscriber **Of Interest** entries:

1. Log in to the server with SSH access as either the **root** user, the **ctmusr** user, or a user that has been added to the **ctmgrp** group.
2. Go to the **/opt/ctm/conf** directory and create a backup of the **of-interest-subscribers.csv** configuration file with the following command:

   ```
   cp of-interest-subscribers.csv of-interest-subscribers.backup.csv
   ```

3. In a text editor, open the **of-interest-subscribers.csv** configuration file and add your **Of Interest** entries at the end of the file. For more information, see "Updating the of-interest-subscribers Configuration File".
4. Save the file.
5. Restart the Charging Traffic Monitor session streaming job service by doing one of the following:
   - If you are the **root** user, run the following command:

     ```
     systemctl restart ctm-spark-session-streaming-job
     ```

   - If you are the **ctmusr** user or a user that has been added to the **ctmgrp** group, run the following command:

     ```
     sudo systemctl restart ctm-spark-session-streaming-job
     ```

Updating the of-interest-subscribers Configuration File

The **of-interest-subscribers** configuration file is in a comma separated values (CSV) format as follows:

```
#Configuration file to hold a list of of-interest subscriber.
#This file is a list comma-separate-value and the columns are as described below
.
#subscriber-id-type is one of these values
# * END_USER_E164
# * END_USER_IMSI
# * END_USER_SIP_URI
# * END_USER_NAI
# * END_USER_PRIVATE
#Subscriber_ID_Type, Subscriber_ID_Data
```

The format to add an **Of Interest** subscriber is a line that contains two parameters separated by a comma:

```
END_USER_E164, 33678012345
```

To update the **of-interest-subscribers.csv** configuration file:

1. For the **Subscriber_ID_Type** parameter, enter one of the following values:
   - END_USER_E164, which adds a subscription to AVP 443 (Subscription-Id) for Subscription-Id-Type 0.
   - END_USER_IMSI, which adds a subscription to AVP 443 (Subscription-Id) for Subscription-Id-Type 1.
   - END_USER_SIP_URI, which adds a subscription to AVP 443 (Subscription-Id) for Subscription-Id-Type 2.
   - END_USER_NAI, which adds a subscription to AVP 443 (Subscription-Id) for Subscription-Id-Type 3.
   - END_USER_PRIVATE, which adds a subscription to AVP 443 (Subscription-Id) on Subscription-Id-Type 4.
2. For the **Subscriber_ID_Data** parameter, enter a string value that matches the **Of Interest** session AVP information:
   - An example of the value for END_USER_E164 is: **`33678012345`**
   - An example of the value for END_USER_IMSI is: **`208017102012345`**
   - An example of the value for END_USER_SIP_URI is: **`sip:234150999999999@ims.mnc015.mcc234.3gppnetwork.org`**
   - An example of the value for END_USER_NAI is: **`fred.smith@example.com`**
   - The value for END_USER_PRIVATE is a string based on the credit-control server's private identifier.

Changing the Display of the Service Type

You can change the display of the Service Type in Charging Traffic Monitor, which is used for filtering the **Latency**, **Transaction Volume**, and the **Transaction Result Code** charts and the **Per Session Display** table.

To change the display of the service type:

1. Log in to the server with SSH access as either the **root** user, the **ctmusr** user, or a user that has been added to the **ctmgrp** group.

2. Go to the **/opt/ctm/conf** directory and create a backup of the **service_type.csv** configuration file with the following command:

   ```
   cp service_type.csv service_type.backup.csv
   ```

3. In a text editor, open the **service_type.csv** configuration file and update the list of service types and their equivalent product type at the end of the file. For more information, see "Updating the service_type Configuration File".

4. Save the file.

5. Go to **/opt/ctm/bin/** and load the data into the database by running the following command:

   ```
   ./config_tac.sh /opt/ctm/conf/service_type.csv
   ```

6. (Optional) Open the **/opt/ctm/conf/config_st.log** file and verify that the service type is up and running.

Updating the service_type Configuration File

The **service_type** configuration file is in a comma separated values (CSV) format as follows:

```
#Configuration file to hold a list of service types provided by the user.
#This file is a list of comma-separate-value and the columns are as described
below.
#service_context_id -- This should be a string
#service_identifier -- This should be a number
#rating_group -- This should be a number
#product_type -- This should be a string
#event_type -- This should be a string
#service_context_id,service_identifier,rating_group,product_type,event_type
#Example -- 32251@3gpp.org,1,1,TelcoGsm,Data
#Example -- 32251@3gpp.org,1,2,TelcoGsm,DataVideo
```

The format to add a service type is a line that contains five parameters separated by a comma. If a comma is part of any value, enclose the value within double quotes:

```
32251@3gpp.org,1,1,TelcoGsm,Data
```

To update the **service_type.csv** configuration file:

1. For the **Service_Context_Id** parameter, enter the Service-Context-Id AVP value sent in the Diameter message (AVP Code 461). Null is an acceptable value if the field is not expected to be present on the credit-control request (CCR).

2. For the **Service_Identifier** parameter, enter the Service-Identifier AVP value sent in the Diameter message (AVP Code 439). Null is an acceptable value if the field is not expected to be present on the CCR.

3. For the **Rating_Group** parameter, enter the Rating-Group AVP value sent in the Diameter message (AVP Code 432). Null is an acceptable value if the field is not expected to be present on the CCR.

4. For the **Product_Type** parameter, enter the product type you have defined for the event in its associated request specification.

5. For the **Event_type** parameter, enter the event type you have defined for the event in its associated request specification.

Changing the Display Name in the Session Results Table IMEISV-TAC Column

You can change the display name from digits to a recognizable device name in the IMEISV-TAC column in the **Session Results** table in Charging Traffic Monitor. The international mobile equipment identity and software version (IMEI_SV) protocol identifies user equipment. IMEI has the following format:

- Type Allocation Code (TAC), which is 8 digits that explains the device type, approved governing body, and manufacture and assembler of the device.
- Serial Number (SN), which is 6 digits that uniquely identifies the device.
- Check Digits/Spare Digit (CD/SD), which is used to avoid a transmission error.
- Software Version Number (SVN), which identifies the software version used by the device.

> **Note:** The IMEISV-TAC column in the **Session Results** table displays only the TAC and SVN digits, formatted as TAC:SVN.

To change the display name of the **Session Results** table's IMEISV-TAC column:

1. Log in to the server with SSH access as either the **root** user, the **ctmusr** user, or a user that has been added to the **ctmgrp** group.
2. Go to the **/opt/ctm/conf** directory and create a backup of the **imeisv_tac.csv** configuration file with the following command:

   ```
   cp imeisv_tac.csv imeisv_tac.backup.csv
   ```

3. In a text editor, open the **imeisv_tac.csv** configuration file and update the TAC-SV parameters at the end of the file. For more information, see "Updating the imeisv_tac Configuration File".
4. Save the file.
5. Go to **/opt/ctm/bin/** and load the data into the database by running the following command:

   ```
   ./config_tac.sh /opt/ctm/conf/imeisv_tac.csv
   ```

6. (Optional) Open the **/opt/ctm/conf/config_tac.log** file and verify that the service is up and running.

Updating the imeisv_tac Configuration File

The **imeisv_tac** configuration file is in a comma separated values (CSV) format as follows:

```
#Configuration file to hold a list of imeisv provided by the user.
#This file is a list of comma-separate-value and the columns are as described
below.
#TAC   -- This should be a String
#SV    -- This should be a String
#NAME  -- This should be a String
#TAC,NAME,SV
#Example -- 1254200,Apple - iPhone 4,00
```

The format is a line that contains three parameters separated by a comma. If a comma is part of any value, enclose the value within double quotes:

```
1254200,Apple - iPhone 4,00
```

To update the **imeisv_tac.csv** configuration file:

1. For the **TAC** parameter, enter the type approval code.
2. For the **SV** parameter, enter the software version number of the device.
3. For the **NAME** parameter, enter a general name for the device that is used, such as, Apple, Samsung, or Google.

Changing the Duration Time Between Each Time Slot in the Session Duration Chart

You can change the duration time between each **Time Slot** in the **Session Duration** chart in Charging Traffic Monitor.

To change the duration time between each **Time Slot** in the session duration chart:

1. Log in to the server with SSH access as either the **root** user, the **ctmusr** user, or a user that has been added to the **ctmgrp** group.
2. Go to the **/opt/ctm/conf** directory and create a backup of the **batch.properties** configuration file with the following command:

   ```
   cp batch.properties batch.properties.backup
   ```

3. In a text editor, open the **batch.properties** configuration file and update the **session.duration.slots** parameter. For more information, see "Updating the session.duration.slots Parameter".
4. Save the file.
5. Restart the Charging Traffic Monitor batch job service by doing one of the following:
   - If you are the **root** user, run the following command:

     ```
     systemctl restart ctm-spark-batch-job
     ```

   - If you are the **ctmusr** user or a user that has been added to the **ctmgrp** group, run the following command:

     ```
     sudo systemctl restart ctm-spark-batch-job
     ```

Updating the session.duration.slots Parameter

The **session.duration.slots** parameter consists of a value and unit separated by a comma:

```
#Session duration KPI time slots in milliseconds
session.duration.slots=5ms,10ms,20ms,50ms,100ms,250ms,500ms,1000ms,2s,5s,10s,30s,6
0s,2m,5m,15m,30m,60m,2h,4h,12h,24h,2d,3d,7d,2w,3w,4w,5w
```

Valid units are:

- ms: milliseconds
- s: seconds
- m: minutes
- h: hours
- d: days
- w: weeks

Changing the Timeout Duration for a Diameter Session

You can change the default timeout duration of a Diameter Session. Timeout is the maximum length of time allowed since the last transaction of an active Diameter session before the session is terminated.

To change the timeout duration for a Diameter session:

1. Log in to the server with SSH access as either the **root** user, the **ctmusr** user, or a user that has been added to the **ctmgrp** group.
2. Go to the **/opt/ctm/conf** directory and create a backup of the **batch.properties** configuration file with the following command:

   ```
   cp batch.properties batch.properties.backup
   ```

3. In a text editor, open the **batch.properties** configuration file and update the **session.timeout.seconds** parameter. For more information, see "Updating the session.timeout.seconds Parameter".
4. Save the file.
5. Restart the Charging Traffic Monitor batch job service by doing one of the following:
   - If you are the **root** user, run the following command:

     ```
     systemctl restart ctm-spark-batch-job
     ```

   - If you are the **ctmusr** user or a user that has been added to the **ctmgrp** group, run the following command:

     ```
     sudo systemctl restart ctm-spark-batch-job
     ```

Updating the session.timeout.seconds Parameter

The **session.timeout.seconds** parameter value is in seconds. The unit is not required:

```
#Session timeout in seconds
# ex. 21600 = 6 hrs
session.timeout.seconds=21600
```

Increasing the Number of Tracked Diameter Transactions in a Session

You can increase the number of tracked **initiate** and **terminate** Diameter transactions in a session for performance testing.

> **Note:** Oracle does not recommend increasing the number of tracked Diameter transactions in a session unless for testing purposes, as this decreases the performance.

To increase the number of tracked Diameter transactions in a session:

1. Log in to the server with SSH access as either the **root** user, the **ctmusr** user, or a user that has been added to the **ctmgrp** group.
2. Go to the **/opt/ctm/conf** directory and create a backup of the **batch.properties** configuration file with the following command:

   ```
   cp session-streaming.properties session-streaming.properties.backup
   ```

3. In a text editor, open the **session-streaming.properties** configuration file and update the **session.max.initiate.terminate.transactions** parameter. For more information, see "Updating the session.max.initiate.terminate.transactions Parameter".
4. Save the file.
5. Restart the Charging Traffic Monitor session streaming job service by doing one of the following:
   - If you are the **root** user, run the following command:

     ```
     systemctl restart ctm-spark-session-streaming-job
     ```

   - If you are the **ctmusr** user or a user that has been added to the **ctmgrp** group, run the following command:

     ```
     sudo systemctl restart ctm-spark-session-streaming-job
     ```

Updating the session.max.initiate.terminate.transactions Parameter

The **session.timeout.seconds** parameter accepts numeric values:

```
#Maximum number of Initiate and Terminate transactions to track per-session.
session.max.initiate.terminate.transactions=5
```

> **Note:** A value of `0` denotes that there is no limit on the number of tracked **initiate** and **terminate** transactions.

Setting the Charging Traffic Monitor KPI Data Retention Time

Your KPI storage requirements depends on your subscriber network. You can change the default KPI data retention time whenever more or less storage is required.

Verifying Current Usage

> **Note:** The following SQL queries can be used to identify the size of your current data. The results will help you estimate the table storage management retention period you require.

To verify your current usage:

1. Log in to Oracle database with Charging Traffic Monitor system administrator credentials.
2. Do one or more of the following:
   - For estimating the table size for each aggregation level of stored KPI's, run the following command:

     ```
     select table_name, num_rows, avg_row_len, num_rows*avg_row_len/1024/1024 as
     storage_space_MB from user_tables where table_name like 'KPI%';
     ```

   - For estimating the table size for **Of Interest** sessions, run the following command:

     ```
     select table_name, num_rows, avg_row_len, num_rows*avg_row_len/1024/1024 as
     storage_space_MB from user_tables where table_name like 'MSG%';
     ```

Note: The storage occupancy given by the above SQL queries are based on the average row length. The space occupied on disk may be different based on the segment allocation.

Updating the Charging Traffic Monitor Data Retention Time

To update the Charging Traffic Monitor data retention time:

1. Log in to the server with SSH access as either the **root** user, the **ctmusr** user, or a user that has been added to the **ctmgrp** group.
2. Go to the **/opt/ctm/conf** directory and create a backup of the **storage.csv** configuration file with the following command:

   ```
   cp storage.csv storage.backup.csv
   ```

3. In a text editor, open the **storage.csv** configuration file and update the storage parameters. For more information, see "Updating the storage Configuration File".
4. Save the file.
5. Go to **/opt/ctm/bin/** and update the data in the database by running the following command:

   ```
   ./config_storage.sh /opt/ctm/conf/storage.csv
   ```

6. (Optional) Open the **/opt/ctm/conf/config_storage.log** file and verify that the storage service is up and running.

Updating the storage Configuration File

The **storage** configuration file is in a comma separated values (CSV) format as follows:

```
#Configuration file to hold a list of storage management table configuration
provided by the user.
#This file is a list of comma-separate-value and the columns are as described
below.
#table_name -- This should be a string
#description -- This should be a string
#drop_interval_schedule -- This should be a number
#interval_unit_schedule -- This should be a string
#drop_interval_random -- This should be a number
#interval_unit_random -- This should be a string
#table_name,description,drop_interval_schedule,interval_unit_schedule,drop_
interval_random,interval_unit_random
#KPI_TX_SEC,Secondly aggregated data for transaction KPIs,21,DAY,7,DAY
#KPI_TX_MIN,Minutely aggregated data for transaction KPIs,3,MONTH,1,MONTH
#KPI_TX_HOUR,Hourly aggregated data for transaction KPIs,2,YEAR,1,YEAR
#KPI_TX_DAY,Daily aggregated data for transaction KPIs,10,YEAR,5,YEAR
#KPI_SESSION_SEC,Secondly aggregated data for session KPIs,21,DAY,7,DAY
#KPI_SESSION_MIN,Minutely aggregated data for session KPIs,3,MONTH,1,MONTH
#KPI_SESSION_HOUR,Hourly aggregated data for session KPIs,2,YEAR,1,YEAR
#KPI_SESSION_DAY,Daily aggregated data for session KPIs,10,YEAR,5,YEAR
#KPI_STREAM_TRANSACTION,Temporary table for transaction KPIs to enhance streaming
performance,1,DAY,6,HOUR
#KPI_SESSION_DURATION,Session duration KPI data storage,1,YEAR,6,MONTH
#MSG_SESSION,Of-interest session details,7,DAY,15,DAY
#MSG_TRANSACTION,Of-interest transaction details,7,DAY,1,DAY
```

The format is a line that contains six parameters separated by a comma. If a comma is part of any value, enclose the value within double quotes:

```
table_name,description,drop_interval_schedule,interval_unit_schedule,drop_
interval_random,interval_unit_random
```

To update the **storage.csv** configuration file:

1. For the **table_name** parameter, do not change the existing value as it represents the Oracle Database table name. Use the table name as it exists in the example.
2. For the **description** parameter, do not change the existing value as it describes the table.
3. For the **drop_interval_schedule** parameter, enter a value for the maximum data storage period.
4. For the **interval_unit_schedule** parameter, enter the unit value for the **drop_interval_schedule** parameter. Units are HOUR, DAY, MONTH, or YEAR.
5. For the **drop_interval_random** parameter, enter a value for the period of time to store data when the available storage space exceeds 90%.
6. For the **interval_unit_random** parameter, enter the unit value for the **drop_interval_random** parameter. Units are HOUR, DAY, MONTH, or YEAR.

Administering the vCollector Probe

The Charging Traffic Monitor system administrator is responsible for the vCollector probe administration tasks.

Verifying the SSL Connection Between the vCollector Probe and Kafka Broker

To verify the SSL connection between the vCollector probe and Kafka broker:

1. Log in to the server with SSH access and that hosts the vCollector probe as the **root** user.
2. Run the following command:

   openssl s_client -debug -connect *ctm_server_name*:**9093 -tls1**

   Where *ctm_server_name* is the host name of the server that hosts Oracle Database and Weblogic Server.

An example command print output that includes the server's certificate is as follows:

```
     -----BEGIN CERTIFICATE-----
    {variable sized random bytes}
     -----END CERTIFICATE-----
    subject=/C=US/ST=CA/L=Santa Clara/O=org/OU=org/CN=firstname lastname
issuer=/C=US/ST=CA/L=SantaClara/O=org/OU=org/CN=kafka/emailAddress=test@abc.com
```

If the certificate does not display or if you receive any other error message then your keystore is not set up correctly.

Administering Oracle Database

The Oracle Database system administrator is responsible for the Oracle Database administration tasks.

Automating Oracle Database Shutdown and Startup with a Linux Service Script

Oracle Database and pluggable databases must be configured to restart all Charging Traffic Monitor resources automatically when the server that hosts Oracle Database is restarted.

To automate Oracle Database shutdown and startup with a service script:

1. Log in to Oracle Database as the Oracle Database system administrator.
2. Go to the **/etc/systemd/system/** directory.
3. Create a file called **oracle-rdbms.service** and add the following lines:

```
[Unit]
Description=The Oracle Database Service
After=syslog.target network.target

[Service]
# systemd ignores PAM limits, so set any necessary limits in the service.
LimitMEMLOCK=infinity LimitNOFILE=65535

#Type=simple
# idle: similar to simple, the actual execution of the service binary is
delayed
# until all jobs are finished, which avoids mixing the status output with shell
output of services.
RemainAfterExit=yes
User=oracle
Group=oinstall
ExecStart=/home/oracle/scripts/startup.sh >> /home/oracle/scripts/startup_
shutdown.log 2>&1 &
ExecStop=/home/oracle/scripts/shutdown.sh >> /home/oracle/scripts/startup_
shutdown.log 2>&1

[Install]
WantedBy=multi-user.target
```

   Where **/home/oracle/** is the Oracle user home directory created during the Oracle Database installation.

4. Save the file.
5. Go to *Oracle_home*/**oracle** and create a scripts directory by running the following command:

```
mkdir -p ./scripts
```

6. In the **scripts** directory create the following script files as follows:
   a. Create a **startup.sh** script file and add the following lines:

```
#!/bin/bash

export TMP=/tmp
export TMPDIR=$TMP
export PATH=/usr/sbin:/usr/local/bin:$PATH
export ORACLE_HOSTNAME=ctm_server_name
export ORACLE_UNQNAME=db12c

export ORACLE_SID=oracle_sid_name
ORAENV_ASK=NO
. oraenv
ORAENV_ASK=YES
```

```
# Start Listener
lsnrctl start
# Start Database

sqlplus / as sysdba << EOF
STARTUP;
EXIT;
EOF
```

Where:

- *ctm_server_name* is the host name of the server that hosts Oracle Database and WebLogic Server.
- *oracle_sid_name* is the Oracle Database system identifier (SID) value entered for the ORACLE_SID environment variable in the **ctm-configuration-param** configuration file.

b. Save the **startup.sh** script file.

c. Create a **shutdown.sh** script file and add the following lines:

```
#!/bin/bash

export TMP=/tmp
export TMPDIR=$TMP
export PATH=/usr/sbin:/usr/local/bin:$PATH
export ORACLE_HOSTNAME=ctm_server_name
export ORACLE_UNQNAME=oracle_unique_name

export ORACLE_SID=oracle_sid_name
ORAENV_ASK=NO
. oraenv
ORAENV_ASK=YES

# Stop Database
sqlplus / as sysdba << EOF
SHUTDOWN IMMEDIATE;
EXIT;
EOF

# Stop Listener
lsnrctl stop
```

Where *oracle_unique_name* is the unique name for Oracle Database.

d. Save the **shutdown.sh** script file.

e. Set the read and execute permissions of the **scripts** directory and script files by running the following commands:

```
chown oracle.oinstall /home/oracle/scripts
chmod u+x /home/oracle/scripts/startup.sh /home/oracle/scripts/shutdown.sh
chown oracle.oinstall /home/oracle/scripts/startup.sh
/home/oracle/scripts/shutdown.sh
```

7. Load and enable the **oracle-rdbms.service** service by running the following commands:

```
systemctl daemon-reload
systemctl enable oracle-rdbms
systemctl start oracle-rdbms
```

8. (Optional) To check the status of Oracle Database and the **systemd** journal run the following:

```
systemctl status oracle-rdbms
journalctl -f -u oracle-rdbms
```

Automating the Opening of a Pluggable Database when Restarting Oracle Database

If you are using pluggable databases you must create a trigger that will restart your pluggable database when Oracle Database has restarted. The script tells the pluggable database that Oracle Database has restarted and changes the pluggable database from the **mount state** to the **open state**.

To automatically open a pluggable database (PDB) when restarting Oracle Database:

1. Log in to Oracle Database as the Oracle Database system administrator with the following SQL command:

```
sqlplus / as sysdba
```

2. Check the status of the pluggable database by running the following:

```
select name, open_mode from v$pdbs;
```

3. Create a startup pluggable database **Sys.After_Startup** trigger that will automatically restart all your pluggable databases when Oracle Database starts. For example:

```
create or replace trigger Sys.After_Startup
after startup on database
begin
     execute immediate 'alter pluggable database all open';
end;
/
```

Administering WebLogic Server

The Oracle WebLogic Server system administrator is responsible for the WebLogic Server administration tasks.

Replacing Certificates

Enabling the secure sockets layer (SSL) activates the WebLogic Server default **Demo Identity** and **Demo Trust** keystores. After installation, replace these with your own SSL certificates for enhanced security.

For more information on the WebLogic Server demonstration keystores and how to replace them, see the WebLogic Server documentation.

Managing Users

During the Charging Traffic Monitor post-installation configuration task the security role **ctm** and corresponding **ctm-group** group are created for a secure access to Charging Traffic Monitor.

All users belonging to the **ctm-group** group are granted the role **ctm**. Any new Charging Traffic Monitor users must be linked with the **ctm-group** group.

For more information about creating users within groups in the WebLogic Server administration console management tool, see the WebLogic Server documentation.

WebLogic Server Domain Configuration

The Charging Traffic Monitor post-installation configuration task configures the following for the WebLogic Server domain:

1. The datasource **dsCTM** is created.
2. The domain security is configured and the following role and group are created:
   - The security role **ctm**.
   - The group **ctm-group**.
3. The following web artifacts are deployed:
   - The **ctm-serviceapp.war** REST API, which is deployed in the **/opt/ctm/web/** directory, where **/opt/ctm** is the directory in which the Charging Traffic Monitor files are installed.

     Important: The **ctm-serviceapp.war** REST API is not backwards compatible and no other application can be built on top.

   - The **ctm-ui.war** static web resources, which is deployed in the **/opt/ctm/web** directory.
   - The **ctm-sso.war** single sign-on for the REST API and Charging Traffic Monitor user interface, which is deployed in the **/opt/ctm/web** directory.

Automating WebLogic Server Shutdown and Startup with a Linux Service Script

To automate WebLogic Server shutdown and startup with a Linux service script:

1. Log in to WebLogic Server as the WebLogic Server system administrator.
2. Go to the **/etc/systemd/system/** directory.
3. Create a file called **wl-admin.service** and do one of the following:
   - If the **Development** environment option was selected during the WebLogic Server installation, add the following lines:

     ```
     [Unit]
     Description=WebLogic Admin Server
     After=syslog.target network.target

     [Service]
     Environment=DOMAIN_HOME=domain_home/ctmdomain
     ExecStart=domain_home/ctmdomain/bin/startWebLogic.sh
     ExecStop=domain_home/ctmdomain/bin/stopWebLogic.sh
     # ExecStartPost=
     Restart=on-abort
     #User=wluser

     [Install]
     WantedBy=multi-user.target
     ```

     Where *domain_home/ctmdomain* is the full path to the Charging Traffic Monitor directory that contains all the files, such as configuration and script files, for the domain in which Charging Traffic Monitor is installed.

   - If the **Production** environment option was selected during the WebLogic Server installation, add the following lines:

```
[Unit]
Description=WebLogic Admin Server
After=syslog.target network.target

[Service]
Environment=DOMAIN_HOME=domain_home/ctmdomain
Environment=WLS_USER=WL_username
Environment=WLS_PS=WL_password
ExecStart=domain_home/ctmdomain/bin/startWebLogic.sh
ExecStop=domain_home/ctmdomain/bin/stopWebLogic.sh
# ExecStartPost=
Restart=on-abort
#User=wluser

[Install]
WantedBy=multi-user.target
```

Where:

- *WL_username* is the user name that has WebLogic Server administrative privileges.
- *WL_password* is the password for the user name that has WebLogic Server administrative privileges.

4. Save the **wl-admin.service** file.
5. Load and enable the **wl-admin.service** service by running the following commands:

```
systemctl daemon-reload
systemctl enable wl-admin
systemctl start wl-admin
```

6. (Optional) To check the status of WebLogic Server and the **systemd** journal run the following:

```
systemctl status wl-admin
journalctl -f -u wl-admin
```

TroubleShooting the Charging Traffic Monitor Components

This section provides guidelines for troubleshooting problems with the Charging Traffic Monitor components. It includes information about log files, diagnosing common problems, and contacting Oracle support.

Troubleshooting Checklist

When problems occur, it is best to do some troubleshooting before you contact Oracle support:

- You know your installation better than Oracle support does. You know whether anything in the system has been changed, so you are more likely to know where to look first.
- Troubleshooting skills are important. Relying on Oracle support to research and solve all your problems prevents you from being in full control of your system.

If you have a problem with your Charging Traffic Monitor system, ask yourself the following questions because Oracle support will ask them:

- What exactly is the problem? Can you isolate it?

Oracle support needs a clear and concise description of the problem, including when it started to occur.

- What do the log files say?

  This is the first thing that Oracle support asks for. Check the error log file for the component of Charging Traffic Monitor, such as the vCollector probe, in which you are having issues.

- Has anything changed in the system? Did you install any new hardware or new software? Did the network change in any way? Does the problem resemble another one you had previously? Has your system usage recently expanded significantly?

- Is the system otherwise operating normally? Has the response time or the level of system resources changed? Are users complaining about additional or different problems?

Using Error Logs to Troubleshoot Charging Traffic Monitor

The Charging Traffic Monitor error log files provide detailed information about system problems. If you are having a problem with Charging Traffic Monitor, look in the log file for the component of Charging Traffic Monitor, such as the vCollector probe, in which you are having issues.

Charging Traffic Monitor records information about actions performed in the Charging Traffic Monitor user interface in the WebLogic Server log files. See the Oracle WebLogic Server Administration Console Help for more information.

Working with the vCollector Probe Logs

The vCollector probe consists of one Linux **systemd** service named **pld-rat**. If the vCollector probe is working no errors are displayed in the **pld-rat** logs.

Example of a **pld-rat** error message:

```
Dec 12 16:01:31 f95f7f9c4a77 rat[885]: ERROR  [KAFKA_PUB_000] FAIL
ssl://ctm:9093/1001: Receive failed: No error.
Dec 12 16:01:31 f95f7f9c4a77 rat[885]: ERROR  [KAFKA_PUB_000] some error: -195
Dec 12 16:01:31 f95f7f9c4a77 rat[885]: ERROR  [KAFKA_PUB_000] some error: -187
```

For additional information about the root cause of a KAFKA_PUB_000 error type, see the **RdKafka::ErrorCode** class in the librdkafka **rdkafkacpp.h** Reference documentation.

Working with the Charging Traffic Monitor Logs

The Charging Traffic Monitor processing engine consists of the following Linux **systemd** services:

- **ctm-ignite**, which is a service that manages the Apache Ignite cache.
- **ctm-kafka**, which is a service that manages the Apache Kafka broker.
- **ctm-spark-batch-job**, which is a service that manages the **Batch Processing Job** feature.
- **ctm-spark-master**, which is a service that manages the Apache Spark master.
- **ctm-spark-session-streaming-job**, which is a service that manages the **Session Streaming Job** feature.
- **ctm-spark-slave**, which is a service that manages Apache Spark workers.

- **ctm-spark-transaction-streaming-job**, which is a service that manages the **Transaction Streaming Job** feature.
- **ctm-zookeeper**, which is a service that manages Apache Zookeeper (required by Kafka broker).

Following are examples of **systemd** commands that verify the status and logs of each service:

- To verify the service status, run one of the following commands:
  - If you are the **root** user, run the following command:

    systemctl status *service_name*

    Where *service_name* is the name of the Linux **systemd** service.
  - If you are the **ctmusr** user, run the following command:

    sudo systemctl status *service_name*

- To restart a service:
  - If you are the **root** user, run the following command:

    systemctl restart *service_name*

  - If you are the **ctmusr** user, run the following command:

    sudo systemctl restart *service_name*

- To verify the service logs, run the following command as the **root** user:

  journalctl -f -u service-name

For more information on the **systemctl** and **journalctl** commands, run the following commands:

```
systemctl --help
journalctl --help
```

Working with Oracle Database Logs

Oracle Database tables whose name starts with ERR are used for logging any exception that occurs in the Oracle Database.

For all other Oracle Database generic issues look in the ERROR_LOG file.

The following is a list of ERR tables:

- ERR_KPI_TRANSACTION, use for issues with transaction KPI inserts.
- ERR_KPI_SESSION, use for issues with session KPI inserts.
- ERR_MSG_SESSION, use for issues with **of-interest** session inserts.
- ERR_SERVICE_TYPE, use for issues with service type master data inserts.
- ERR_DFE_NL, use for issues with the Diameter Front End or the Network Location master data inserts.
- ERR_ST_RC_COMBINATIONS, use for issues with the service type Result code combination master data inserts.
- ERR_IMEISV, use for issues with the IMEI-SV master data inserts.
- ERR_REALMS_IMEISV, use for issues with DFE or NL realms and IMEI-SV together with master data inserts.

Monitoring and Troubleshooting Oracle Database

1. Log in to the server that hosts Oracle Database and WebLogic Server as the user that has full SYSDBA privileges for local database access.
2. Initialize the Oracle wallet by running the following command:

   ```
   . /opt/ctm/scripts/ctm-configuration-param
   ```

3. Connect to the Charging Traffic Monitor PDB database container by running the following command:

   ```
   sqlplus /@$ORACLE_PDB
   ```

4. Do one or more of the following:

   - To return all errors that have been raised during the running of Oracle Database, run the following SQL command:

     ```
     select * from error_log order by created_date desc;
     ```

   - To return errors that are specific to an ERR table, run the following SQL command:

     ```
     select * from ERR_table;
     ```

     Where *ERR_table* is the name of an Oracle Database ERR table that is listed above.

Monitoring Tablespace Usage

To monitor tablespace usage:

1. Log in to the server that hosts Oracle Database and WebLogic Server as the user that has full SYSDBA privileges for local database access.
2. Initialize the Oracle wallet by running the following command:

   ```
   . /opt/ctm/scripts/ctm-configuration-param
   ```

3. Connect to the Charging Traffic Monitor PDB database container by running the following command:

   ```
   sqlplus /@$ORACLE_PDB
   ```

4. Monitor the tablespace usage by running the following:

   ```
   SELECT a.TABLESPACE_NAME, total,
   free,
   ROUND(100*(1-free/total),1) pct_usage
   FROM
   (SELECT TABLESPACE_NAME,
   SUM(BYTES) total
   FROM dba_data_files
   GROUP BY TABLESPACE_NAME
   ) a ,
   (SELECT TABLESPACE_NAME,
   SUM(BYTES) free
   FROM dba_free_space
   GROUP BY TABLESPACE_NAME
   ) b
   WHERE a.TABLESPACE_NAME=b.TABLESPACE_NAME(+);
   ```

5. Exit SQL.

Example command print output as follows:

```
TABLESPACE_NAME                 TOTAL          FREE        PCT_USAGE
------------------------------ ----------     ----------   ----------
SYSAUX                          629145600       40501248         93.6
TSCTM01                        1.0737E+10     1.0314E+10          3.9
USERS                          2469396480     2466775040           .1
SYSTEM                          325058560        1966080         99.4
EXAMPLE                        1304166400       25952256           98
TSCTM03                        1.0737E+10     1.0322E+10          3.9
TSCTM02                        1.0737E+10     1.0297E+10          4.1
TSCTMIDX                       1.0737E+10     1.0647E+10           .8
TSCTM04                        1.0737E+10     1.0297E+10          4.1
TSSESSION                      2.1475E+10     2.1260E+10            1
10 rows selected.
```

For information on how to identify your current data storage, see "Verifying Current Usage".

Working with WebLogic Server Logs

The logs relative to the Charging Traffic Monitor interface are available using the Weblogic Server console access. For more information, see the Weblogic Server documentation.

Diagnosing Charging Traffic Monitor User Interface Problems

Charging Traffic Monitor user interface problems can be diagnosed with the WebLogic Server Diagnostic Framework, which enables the collection, archiving, and access diagnostic information about applications hosted on WebLogic Server. See the Oracle WebLogic Server Administration Console Help for more information.

This section lists some common Charging Traffic Monitor problems and describes how to diagnose the error messages and resolve the problems.

Refreshing the Browser

Do not refresh your browser.

Refreshing the browser causes unpredictable problems in the Charging Traffic Monitor user interface.

Unable to Perform Any Task after Logging In

If after you log in to Charging Traffic Monitor the links in the navigation list are not displayed or you cannot perform any task. Contact your system administrator and verify that you are a user in the WebLogic Server **Config Admin** group.

Trouble Viewing Data in Charging Traffic Monitor

If after you log in to Charging Traffic Monitor you cannot view any data (even existing historical data). This could be due to some Charging Traffic Monitor services being out of synchronization. Restart the WebLogic Server server on which Charging Traffic Monitor is deployed, which synchronizes the data.

Diagnosing vCollector Probe Problems

The vCollector probe contains a utility tool that displays Diameter message packet counters received from your online charging system (OCS) and after **rat** and **panther** processing. For more information on how to use the **rat_mon.py** tool, see "Working

with the vCollector Probe Troubleshooting Utility".

Diagnosing Charging Traffic Monitor Processing Engine Problems

You can monitor the Charging Traffic Monitor processing engine with the following URLs:

- The Spark master URL, which lists all the Spark jobs that are running:

  http://*ctm_server_name*:8080/

  Where *ctm_server_name* is the host name of the server that hosts Oracle Database and Weblogic Server.

- Transaction Streaming Job:

  http://*ctm_server_name*:4040/streaming/

- Session Streaming Job:

  http://*ctm_server_name*:4041/streaming/

- Batch Processing Job:

  http://*ctm_server_name*:4042/jobs/

For more information on the Spark web user interface, see the Apache Spark documentation.

Getting Help for Charging Traffic Monitor Problems

If you cannot resolve a Charging Traffic Monitor problem, contact Oracle support.

Before you contact Oracle support, try to resolve the problem with the information contained in the Charging Traffic Monitor component's a log file. For more information, see "Using Error Logs to Troubleshoot Charging Traffic Monitor". If this does not help resolve the problem, collect the following information:

- A clear and concise description of the problem, including when it started to occur.
- Relevant portions of the relevant log files.
- Relevant configuration files.
- Recent changes in your system after which the problem occurred, even if you do not think they are relevant.
- A list of all Charging Traffic Monitor components and patches installed on your system.

When the list is complete, report the problem to Oracle support.

Known Problems

This section describes the known problems when installing Charging Traffic Monitor.

ORA-01034 Error when the Wrong ORACLE_SID Value is Entered

The following ORA-01034 error is displayed when you have entered an incorrect value for the ORACLE_SID environment variable in the **ctm-configuration-param** configuration file during the post-installation of Charging Traffic Monitor.

```
CREATE USER CTM
*ERROR at line 1:
ORA-01034: ORACLE not available
```

```
Process ID: 0
Session ID: 0 Serial number: 0
```

Solution: Verify the Oracle Database system identifier (SID) name and replace the incorrect value with the correct value in the **ctm-configuration-param** configuration file. Re-run the **`./ctm-configuration`** command.

User Error when Entering the Wrong SSL Values

The following errors are displayed when you have entered one or more values incorrectly for the SSL environment variables in the **rat.conf** configuration file during the post-installation of the vCollector probe.

```
Dec 28 15:02:10 vCollector systemd[1]: Starting CTM Probe...
Dec 28 15:02:10 vCollector system_layout.py[26361]: missing driver option of
[dpdk] section in /etc/iptego/rat.conf
Dec 28 15:02:10 vCollector systemd[1]: pld-rat.service: main process exited,
code=killed, status=11/SEGV
Dec 28 15:02:10 vCollector systemd[1]: Failed to start CTM Probe.
```

Solution: Verify the **ssl_key**, **ssl_key_pw**, **ssl_cert**, and **ssl_cas** values and replace any incorrect values with the correct value in the **rat.conf** configuration file. Re-run the **`systemctl start pld-rat`** command.

Secure Deployment Checklist

To deploy Charging Traffic Monitor securely, follow this checklist:

1. Pre-Installation steps:
   a. Enable secure sockets layer (SSL) for the WebLogic Server domain.
   a. Verify that you have Java 8 with the latest security update installed and configured with your WebLogic Server installation.
   b. Configure the server keystore certificate, and obtain the client keystore trusted certificate.
   c. Configure Oracle Database advanced security encryption and integrity algorithms for a secure connection from the installer.
2. Installation steps:
   a. Select SSL mode, and provide the client keystore certificate (.jsk file) for connecting to WebLogic Server with SSL.
3. Post-Installation steps:
   a. If you do not need the installation log files, delete them.
   b. The WebLogic Server administrator must create the Charging Traffic Monitor users based on the roles and privileges. For more information, see "Managing Users".
   c. Do not use your browser's remember password feature for the WebLogic Server Administration Console user URL.
   d. Enable secure cookies.
   e. Verify that file permissions for the installed files are 600 for all nonexecutable files and 700 for all executable files.
4. Un-installation steps:

a. Delete the log files in the **oraInventory/logs** directory manually if you do not need them, or protect them appropriately if they are required for further installations.

Working with the vCollector Probe Troubleshooting Utility

This section provides guidelines for working with the vCollector probe **rat_mon.py** troubleshooting utility.

The **rat_mon.py** utility displays Diameter message packet counters results after **rat** and **panther** processing.

The utility page displays the following main sections:

- **rat**

  The **rat** process implements the vCollector probe's sniffing and filtering functions.

  For more information, see "Understanding the rat Section".

- **panther**

  The **panther** process implements the vCollector probe's Diameter processing function.

  For more information, see "Understanding the panther Section".

Accessing the vCollector Probe Utility

To access the vCollector Probe utility:

1. Log in to the server that hosts the vCollector probe with administrative privileges.
2. Go to the **/usr/share/pld/rat/** directory.
3. Open the **rat_mon.py** utility by running the following command:

   ```
   ./rat_mon.py
   ```

4. Navigate inside the **rat_mon.py** page by selecting the following keyboard shortcuts:
   - To quit the utility, select **q**.
   - To scroll down and up, select **j** to scroll down or **k** to scroll up.

     To scroll down and up in 10 line multiples, select **shift+ j** (J) to scroll 10 lines down or **shift+k** (K) to scroll 10 lines up.
   - To update the page, select **u**.
   - To go to the next page, select the **Tab** key.
   - To toggle between the following statistics:
     - To display worker statistics, select **1**.
     - To display analyzer statistics, select **2**.
     - To display packet statistics, select **3**.
     - To display publisher statistics, select **4**.

Understanding the rat Section

This section displays the sent Diameter message packet counters by the **rat** processing unit.

The **rat** section contains the following modules:

- Sniffers Module
- Filters Module
- Packet Publishers Module

Sniffers Module

The **sniffers** module displays the input sniffer status. There is one statistic line for each sniffer defined in the **rat.conf** configuration file.

Table 6–1 describes the **sniffers** module counters.

Table 6–1 Sniffers Module

Counter	Description
pps	The number of packets for each second captured by the sniffer.
received	The cumulated number of packets captured by a sniffer since the last restart of the **rat** process.
dropped	The number of packets dropped by a sniffer since the last restart of the **rat** process.
in_queue	The number of packets inside the sniffer queue.
cpu	The CPU identifier used by a sniffer.
Bps	The number of bytes for each second captured by the sniffer.
bytes	The cumulated number of bytes captured by a sniffer since the last restart of the **rat** process.

Filters Module

The **filters** module displays the processing status after a filter rule is applied. The filter rule is defined in the **rat.conf** configuration file. For example:

```
############## panther section ######################
[panther]
filter = ((tcp or sctp) and (port 3868)) or (vlan and ((tcp or sctp) and (port
3868))
```

For more information on the **rat.conf** configuration file, see "rat.conf Configuration File Parameters".

Table 6–2 describes the **filters** module counters.

Table 6–2 Filters Module

Counter	Description
pps	The number of packets for each second that match a filter rule.
received	The cumulated number of packets that match a filter rule since the last restart of the **rat** process.
dropped	The number of packets dropped by a filter rule since the last restart of the **rat** process.
in_queue	The number of packets inside a filter processing queue.

Table 6–2 (Cont.) Filters Module

Counter	Description
cpu	The CPU identifier used by the filter process.

Packet Publishers Module

The **packet publishers** module displays the processing status before the packet is sent to the Diameter transactions management tool for processing. Historically this is known as **panther**.

Table 6–3 describes the **packet publishers** module counters.

Table 6–3 Packet publishers Module

Counter	Description
dropped	The number of packets dropped between the **rat** processing and the **panther** processing unit.
in_queue	The number of packets inside a queue between the **rat** processing and the **panther** processing unit.
recieved	The number of packets received by the **rat** processing.
sent	The number of packets that are sent to the **panther** processing unit.
sent_other	The number of other transport layer packets.
sent_rudp	The number of sent reliable user datagram protocol (RUDP) packets.
sent_sctp	The number of sent stream control transmission protocol (SCTP) packets.
sent_tcp	The number of sent transmission control protocol (TCP) packets.
sent_udp	The number of sent user datagram protocol (UDP) packets.

Understanding the panther Section

This section displays the received Diameter message packet counters by the **panther** processing unit.

The **panther** section contains the following modules:

- Receiver Module
- Correlator Module
- Publishers Module
- Kafka Module

Receiver Module

The **receiver** module displays the network packets received by the Diameter management module.

Table 6–4 describes the **receiver** module counters.

Table 6–4 Receiver Module

Counter	Description
drop	The number of packets dropped since the last restart of the **rat** process.
in_queue	The number of packets in the processing queue.

Table 6–4 (Cont.) Receiver Module

Counter	Description
proc	The cumulated number of processed packets.
proc/s	The number of processed packets received for each second.

Correlator Module

The **correlator** module displays the Diameter messages managed by the Diameter management module

Table 6–5 describes the **correlator** module counters.

Table 6–5 Correlator Module

Counter	Description
drop	The number of transactions dropped by a correlator since the last restart of the **rat** process.
in_queue	The number of transactions in the correlator processing queue.
proc	The cumulated number of processed correlator transactions.
proc/s	The number of processed correlator transactions for each second.

Publishers Module

The **publishers** module displays the status of each publisher packet. There is one statistic line for each publisher defined in the **rat.conf** file.

Table 6–6 describes the **publishers** module counters.

Table 6–6 Publishers Module

Counter	Description
transactions	The number of transactions processed by a publisher.
expired	The number of expired published transactions. An expired transaction is either a partially completed transaction or a transaction that did not complete (timed out).

Kafka Module

The **kafka** module displays the Kafka delivery status.

Table 6–7 describes the **kafka** module counters.

Table 6–7 Kafka Module

Counter	Description
delivered	The number of transactions delivered to the Kafka broker.
failed	The number of failures returned by the Kafka interface. For the Oracle Linux service logs run the **journalctl** command as the **root** user. Error codes are created for failures and are found in the **pld-rat** log file. The error code values are defined by **librdkafka**. For more information, see the librdkafka Reference documentation.
dropped	The number of transactions that were dropped and not sent to the Kafka broker.

Table 6–7 (Cont.) Kafka Module

Counter	Description
in_queue	The number of transactions inside the Kafka sending queue.

7

Charging Traffic Monitor Reference

This chapter provides reference information for Oracle Communications Charging Traffic Monitor.

Charging Traffic Monitor Configuration Reference

This section describes reference information for configuring Charging Traffic Monitor:

- The **ctm-configuration-param** configuration file is an environment variable script that contains a list of the environment variables and their values that are required for the Charging Traffic Monitor configuration task. It includes the secure connection credentials for a secure connection between the Charging Traffic Monitor application, the vCollector probe, other Oracle products and third-party products, and your online charging system (OCS).

  See "ctm-configuration-param Configuration File Environment Variables".

- The **rat.conf** configuration file is used by the **pld-rat** service for configuring the vCollector probe for your system.

  See "rat.conf Configuration File Parameters".

ctm-configuration-param Configuration File Environment Variables

Table 7–1 lists the environment variables and default values in the **/opt/ctm/scripts/ctm-configuration-param** configuration file.

Table 7–1 ctm-configuration-param Configuration File

Environment Variable	Default	Description
ORACLE_BASE	$ORACLE_BASE	The root path and directory in which Oracle Database is installed. This directory contains the Oracle Database software and directories, such as, **bin**, **rdbms**, and **sqlplus**.
ORACLE_HOME	$ORACLE_HOME	The path and directory in which Oracle Database is installed. This directory is a subdirectory of ORACLE_BASE containing the installed files and files such as, registry entries, net service names, program groups, and the PATH variable.
ORACLE_SID	$ORACLE_SID	The Oracle System identifier (SID), which is a unique name for identifying a database on a system.

Table 7–1 (Cont.) ctm-configuration-param Configuration File

Environment Variable	Default	Description
ORACLE_PDB	-	The Oracle pluggable database (PDB) name, which contains the Charging Traffic Monitor portable schemas, schema objects, and non schema objects. **Important:** This value must be the *connection_name* value that you entered in the **tnsnames.ora** configuration file. For more information, see "Adding a Connect Descriptor Name for a Pluggable Database".
ORACLE_DB_PORT	1521	The listening port number of Oracle Database.
ORACLE_DB_HOST	localhost	The host name for the server that hosts Oracle Database.
ORACLE_DB_USER	CTM	The user name that was used to install Oracle Database.
ORACLE_WALLET_PATH	/opt/ctm/wallet	The path to the Oracle wallet directory where your Charging Traffic Monitor Oracle wallet files are stored.
ORACLE_WALLET_ADMIN	/opt/ctm/oracle_admin	The path to the directory that contains the **sqlnet.ora** and the **tnsnames.ora** files.
CTM_SERVICE	ORCL	The Charging Traffic Monitor transparent network substrate (TNS) service name. The value is generally the equivalent of ORACLE_PDB.
CTM_CONNECTION_STRING	$ORACLE_DB_HOST/$CTM_SERVICE	The Charging Traffic Monitor database connection string. By default this is initialized using the ORACLE_DB_HOST and CTM_SERVICE values.
CTM_TS_SIZE	75G	Sets the size of each **tsctm** tablespace datafile in the Charging Traffic Monitor database. The **tsctm** Tablespace files are: ■ tsctm01.dbf ■ tsctm01.dbf ■ tsctm02.dbf ■ tsctm03.dbf ■ tsctm04.dbf ■ tsctmidx.dbf **Important:** Do not change this value unless the Oracle Database hardware specification is not followed.
CTM_TS_SESSION	200G	Sets the size of the **tssession.dbf** tablespace datafile in the Charging Traffic Monitor database. **Important:** Do not change this value unless the Oracle Database hardware specification is not followed.
CTM_TS_STORAGE_DIR	$ORACLE_BASE/oradata/$ORACLE_SID/$ORACLE_PDB	The directory in which the Charging Traffic Monitor database tablespace datafiles are stored. The global storage space inside the Charging Traffic Monitor database tablespace directory is 5 times the CTM_TS_SIZE storage size plus the CTM_TS_SESSION size.

Table 7–1 (Cont.) ctm-configuration-param Configuration File

Environment Variable	Default	Description
TNS_ADMIN	$ORACLE_ WALLET_ADMIN	The path and directory in which the SQL *NET configuration files are stored, such as **sqlnet.ora** and **tnsnames.ora**. **Note:** This environment variable locates your Oracle wallets.
JAVA_HOME	/usr/java/default	The path to the directory in which Java is installed.
WL_HOST	localhost	The host name for the server that hosts Oracle Database and WebLogic Server.
WL_USERNAME	weblogic	The user name that has the WebLogic Server user interface portal access privileges.
WL_DOMAIN	mydomain	The WebLogic Server **domains** directory name.
WL_DOMAIN_DIR	$HOME/$WL_ DOMAIN	The full path to the WebLogic Server **domains** directory.
WL_PORT	7001	The listening port number of the WebLogic Server administrative instance.
WL_TARGET	myserver	The name of the WebLogic Server administrative server instance.
WL_HOME	/root/wls12130/	The path to the directory in which WebLogic Server is installed.
ORACLE_DB_SSH_USER	-	(Optional) The secure socket shell (SSH) user name that has Oracle Database remote access privileges. If Oracle Database is not installed on the server that hosts the Charging Traffic Monitor processing engine this name is used.
WL_SSH_USER	-	(Optional) The SSH user name that has WebLogic Server remote access privileges. If WebLogic Server is not installed on the server that hosts the Charging Traffic Monitor processing engine this name is used.
ORACLE_DB_SYSDBA_USER	sys	(Optional) The user name that has full SYSDBA privileges for remote database access. **Note:** If a value is entered, a value is not required for the ORACLE_DB_LOCAL_USER environment variable.
ORACLE_DB_LOCAL_USER	-	The user name that has full SYSDBA privileges for local database access. **Note:** If a value is entered, a value is not required for the ORACLE_DB_SYSDBA_USER environment variable.
BROKER_HOST_NAME	$(hostname)	A unique alias name used by the keytool utility for generating and installing the Kafka broker SSL certificate. This value is initialized by default.
SSL_DIR	$HOME/ctm-ssl	The directory in which the SSL certificate and key files are generated. This value is initialized by default.
SSL_CERTIFICATE	-	(Optional) The name of the SSL certificate.
SSL_CERTIFICATE_VALIDITY_ DAYS	365	(Optional) The number of days the client server stores the SSL certificate before requesting reauthorization.

Table 7–1 (Cont.) ctm-configuration-param Configuration File

Environment Variable	Default	Description
SSL_COUNTRY_NAME	-	(Optional) The country attribute of the server certificate.
SSL_STATE_NAME	-	(Optional) The state or province attribute of the server certificate.
SSL_LOCALITY_NAME	-	(Optional) The locality attribute of the server certificate.
SSL_ORGANIZATION_NAME	-	(Optional) The organization attribute of the server certificate.
SSL_ORG_UNIT_NAME	-	(Optional) The organization unit of the server certificate.
SSL_COMMON_NAME	-	(Optional) The common name of the server certificate.
SSL_EMAIL_ADDRESS	-	(Optional) The email address of the server certificate.

rat.conf Configuration File Parameters

The **rat.conf** configuration file is divided into sections, which are denoted by square brackets and contain one or more assignment statements.

After adjusting the available configuration values for your system you can enable the **pld-rat** service daemon by running the following commands:

```
systemctl enable pld-rat
systemctl start pld-rat
```

Table 7–2 lists the parameters in the **/etc/iptego/rat.conf** configuration file.

Table 7–2 rat.conf Configuration File Parameters

Section	Parameter	Default	Format	Description
[base]	sniffer	-	-	Reserved for internal use. Do not change.
[zmqrpc]	bin_url	-	-	Reserved for internal use. Do not change.
[publisher]	enable_rtcp	-	-	Reserved for internal use. Do not change.
[rtprec]	max_streams	-	-	Reserved for internal use. Do not change.
[sniffer/*sniffer-name*]	type	-	-	Reserved for internal use. Do not change.
[sniffer/*sniffer-name*]	devices	ens3f0 ens3f1	string *device-name* followed by a space.	The list of network device names (*device-name*).
[sniffer/*sniffer-name*]	disable_rtp	-	-	Reserved for internal use. Do not change.
[sniffer/*sniffer-name*]	workers	-	-	Reserved for internal use. Do not change.
[sniffer/*sniffer-name*]	filter_cpus	-	-	Reserved for internal use. Do not change.

Table 7–2 (Cont.) rat.conf Configuration File Parameters

Section	Parameter	Default	Format	Description
[sniffer/*sniffer-name*]	sniffer_cpus	-	-	Reserved for internal use. Do not change.
[sniffer/*sniffer-name*]	blocks	-	-	Reserved for internal use. Do not change.
[sniffer/*sniffer-name*]	snaplen	-	-	Reserved for internal use. Do not change.
[sniffer/*sniffer-name]*	poll_mode	-	-	Reserved for internal use. Do not change.
[panther]	filter	((tcp or sctp) and (port 3868)) or (vlan and ((tcp or sctp) and (port 3868)))	string	Specifies the filtering rule that a packet must fulfill to be categorized into the protocol type of this signaling section. You can see the PCAP packet filters and syntax with the Oracle Linux man page **man pcap-filter** command.
[publisher]	type	-	-	Reserved for internal use. Do not change.
[kafka]	brokers	ctm:9092	string	The Kafka broker URL connection.
[kafka]	topic	-	-	Reserved for internal use. Do not change.
[kafka]	compression	-	-	Reserved for internal use. Do not change.
[kafka]	encryption	ssl code default: plaintext	string	The protocol used for communicating with brokers.
[kafka]	ssl_key	-	string	The client's private key (PEM container format) that is used for authentication.
[kafka]	ssl_key_pw	-	string	The private key passphrase.
[kafka]	ssl_cert	-	string	The client's public key (PEM container format) that is used for authentication.
[kafka]	ssl_cas	-	string	The California certificate file or directory path that verifies the broker's key.
[kafka]	hwm	-	-	Reserved for internal use. Do not change.
[receiver]	workers	-	-	Reserved for internal use. Do not change.
[receiver]	queue_size	-	-	Reserved for internal use. Do not change.
[correlator]	workers	-	-	Reserved for internal use. Do not change.
[correlator]	queue_size	-	-	Reserved for internal use. Do not change.

Table 7–2 (Cont.) rat.conf Configuration File Parameters

Section	Parameter	Default	Format	Description
[correlator]	app_ids	-	-	Reserved for internal use. Do not change.
[status]	publisher_type	-	-	Reserved for internal use. Do not change.
[uuid]	uuid	random UUID For example, `a9f8ae58-0276-11e6-b0c5-28d2445b7569`	string Represents a 128-bit UUID.	The vCollector probe identifier. By default, this section is linked to the **/etc/iptego/psa/probe_uuid.conf** file, which is generated automatically during the vCollector probe RPM installation.